Nothing Funny or Romantic about These RomCom IoCs and Artifacts

Table of Contents

Executive Report

The threat actor dubbed “RomCom,” known for deploying spoofed versions of popular software, has been quite busy these past few months. In the past, he was seen imitating Advanced IP Scanner and PDF Filler. More recently, though, he’s been targeting Ukraine, the U.K., and other English-speaking countries by spoofing SolarWinds, KeePass, PDF Reader Pro, and Veeam.

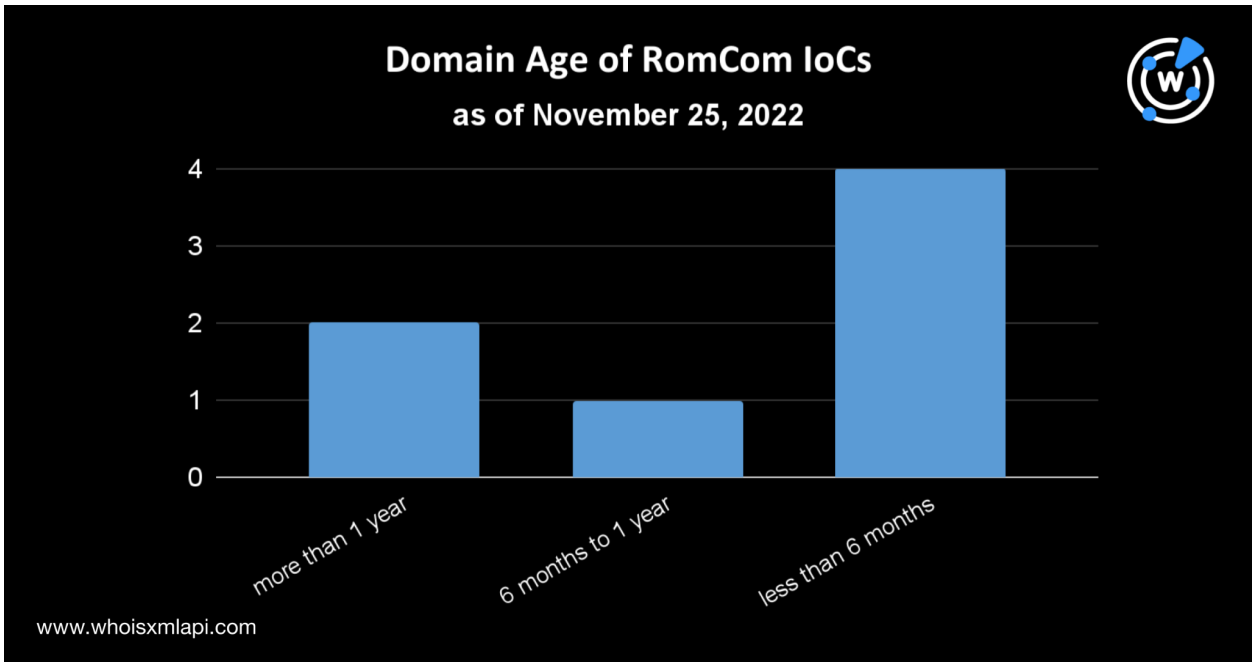
Victims who download the fake tools install a malicious code into their devices that can collect data, take screenshots, and send these to command-and-control (C&C) servers. While RomCom employs sophisticated obfuscation techniques, he may have left some trails. WhoisXML API researchers analyzed published indicators of compromise (IoCs) and expanded the list to find suspicious properties that RomCom or other threat actors may own and could weaponize. Here are some of our key findings.

- Some domains used in RomCom’s campaigns have deep WHOIS histories.
- Almost all the IoCs actively resolved to IP addresses geolocated in the U.S.
- More than 2,600 artifacts connected to the IoCs through WHOIS details, IP resolutions, and targeted software were found.
- About 3% of the artifacts were flagged as malicious, and several unreported ones hosted questionable content.

IoC Analysis

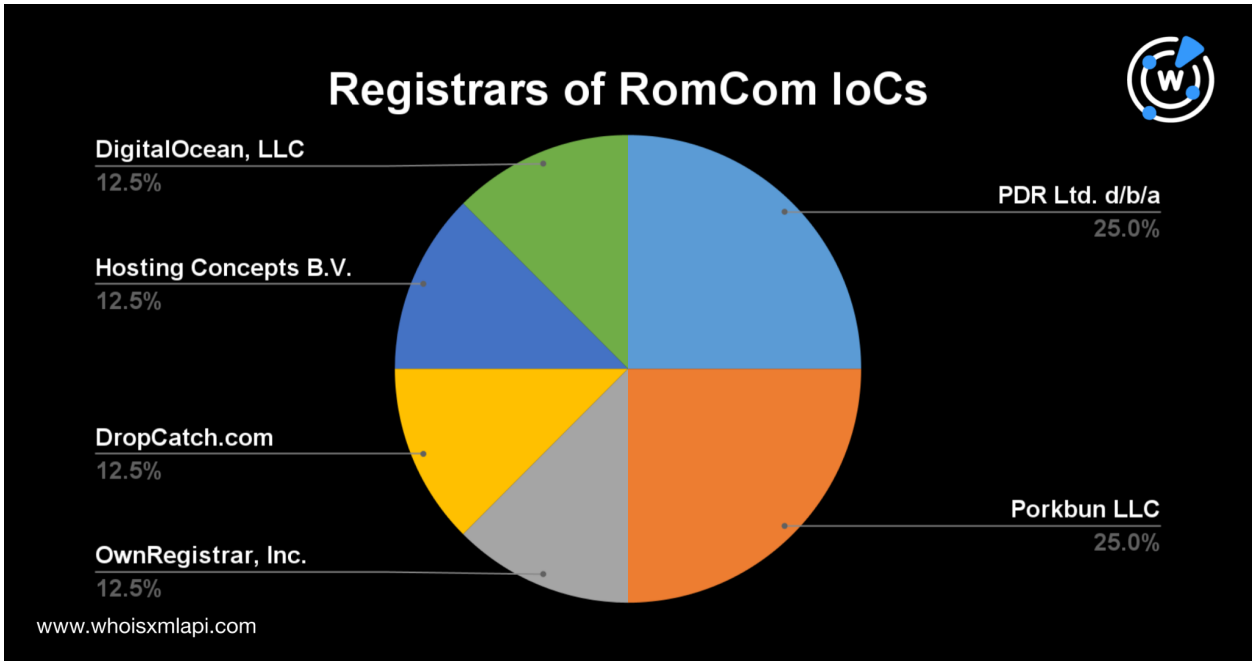
Based on BlackBerry and Palo Alto Network research, we gathered seven domains and one IP address tagged as IoCs related to RomCom. All except one domain fell under the .com top-level domain (TLD). Using WHOIS Search to dig into these properties, we determined the following:

- **Domain age:** While all the malicious domains were newly registered, around the time they were weaponized, three had deep WHOIS histories. The cybersquatting domain advanced-ip-scaner[.]com was initially created in November 2015, while wveeam[.]com was added in August 2017.



- **Ownership:** Two unredacted email addresses were used to register two of the domains. Both of them were proton[.]me email addresses, which also appeared in the WHOIS records of five suspicious domains. The rest of the IoCs' WHOIS records were privacy-protected.

- **Administration:** IoC management fell under the purview of several registrars. Two belonged to PDR Ltd.; another two to Porkbun; and the rest to Hosting Concepts, DropCatch, and OwnRegistrar.



- **Name server (NS):** Only the domains managed by PDR Ltd. recently underwent NS changes—4qzm[.]com currently uses a "transition" NS, while wveeam[.]com utilizes an NS for suspended domains. The rest of the IoCs still used the same NSs from when they were registered.

- **IP resolutions:** All of the IoCs except wveeam[.]com had active IP resolutions mostly geolocated in the U.S. They were assigned to different Internet service providers (ISPs), including Digital Ocean, Linode, and HostWinds.

IoC Expansion: Detecting Suspicious Connected Domains

A deeper investigation led us to more than 2,600 artifacts. We detailed how we retrieved these properties below.

String-Based Expansion

Knowing that RomCom's signature tactic is to spoof well-known software, we looked for possible cybersquatting resources bearing the names of such targets. We retrieved more than 1,200 domains and subdomains added between 1 June and 18 November 2022 broken down into their spoofed targets.

Spoofed Software	Legitimate Website	Search String	Number of Possible Cybersquatting

			Resources
SolarWinds Network Performance Monitor	solarwinds[.]com/network-performance-monitor	“solarwind”	387
KeePass Open-Source Password Manager	keepass[.]info	“keepas”	128
PDF Reader Pro	pdfreaderpro[.]com	“pdfreader”	43
Advanced IP Scanner	advanced-ip-scanner[.]com	“advance + -ip” “-ip + scan”	52
PDF Filler	pdffiller[.]com	“pdf + filler”	52
Veeam Backup and Recovery Software	veeam[.]com	“veeam”	589

Samples of the cybersquatting properties can be found in the Appendix.

DNS-Based IoC Expansion

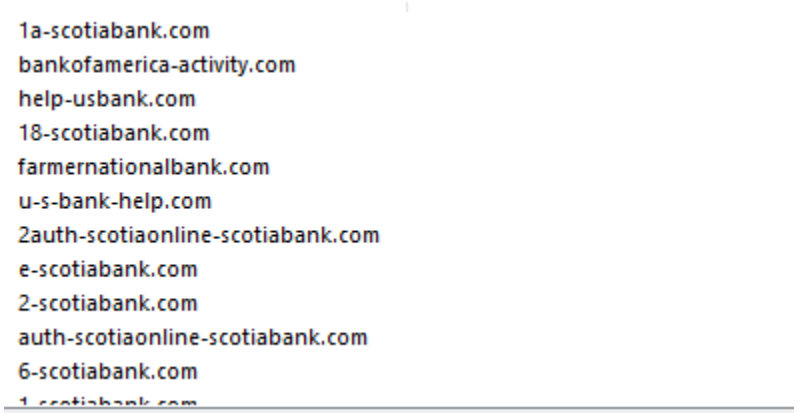
Our DNS analysis on the IoCs revealed five IP hosts, which led us to 832 connected domains after running them through Reverse DNS Search. While some of these properties may be innocently connected to the IP addresses, others appear suspicious.

For instance, we found domains that seem to be spoofing Microsoft Azure, AnyDesk, Google Translate, and Google Analytics.

Expansion Based on Shared WHOIS Record Details

Another method for finding artifacts is through Reverse WHOIS Search. Since the domains registered using the proton[.]me email addresses were managed by PDR Ltd., we used the registrar name and email domain as search strings. We found 641 domains with PDR Ltd. and proton[.]me email addresses.

The WHOIS-connected artifacts turned out to be suspicious, too. For instance, some of them seemed to be spoofing Scotia Bank, Bank of America, and Farmer National Bank, as seen below.



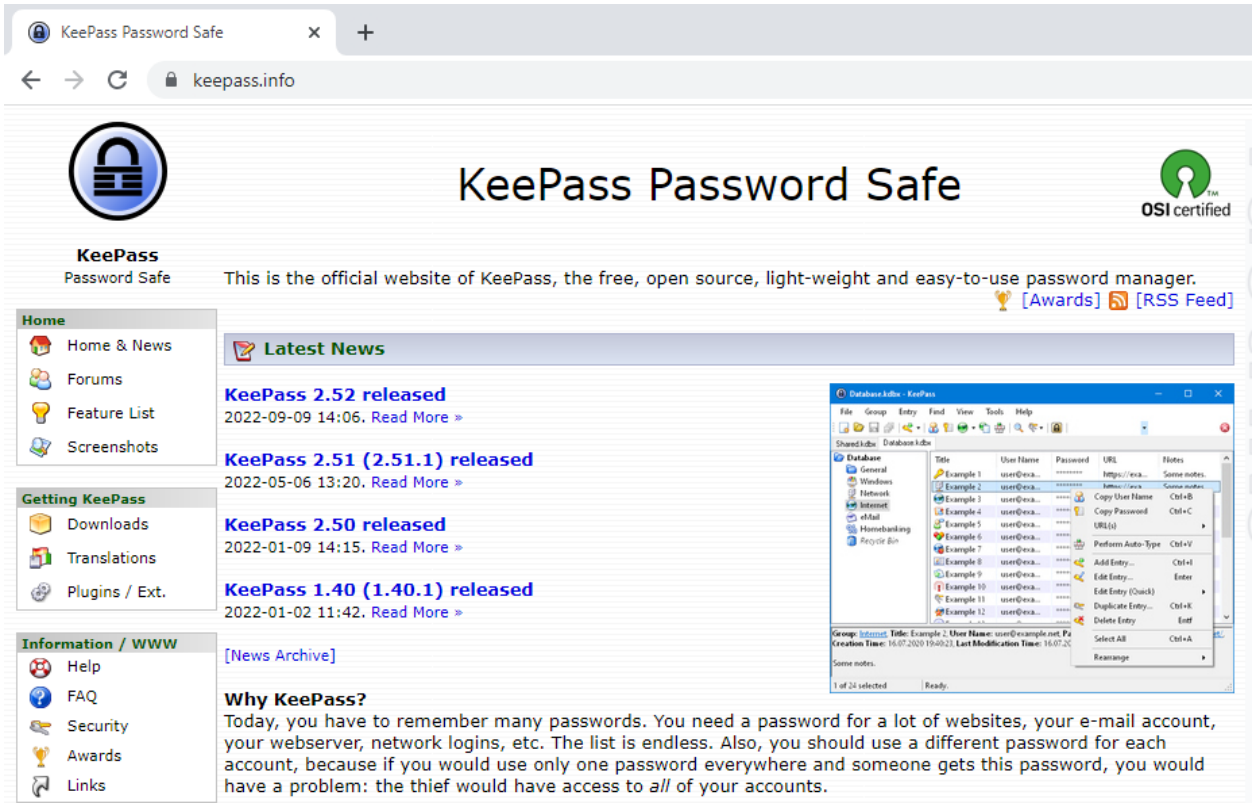
We also found domains consistent with the RomCom IoCs, such as those targeting SolarWinds Network Performance Monitor and Veeam.

Artifact Analysis: Malicious Usage and Web Content

About 3% of the artifacts we discovered turned out to be malicious, most notably:

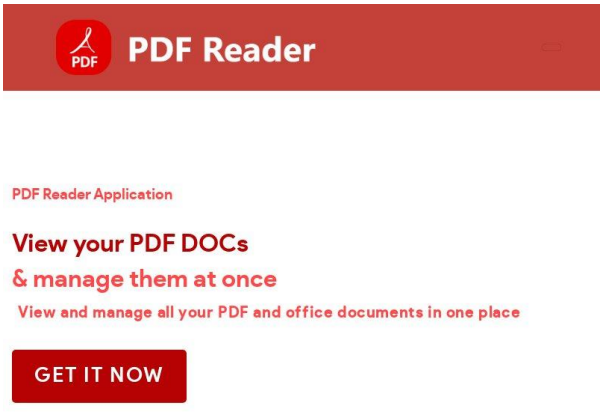
- Digital properties consistent with the RomCom IoCs, such as those targeting PDF Reader and Keepass sporting different TLDs
- Finance-themed properties targeting Bank of America, Chase, Coinbase, and Scotia Bank
- Tech-related domains spoofing virtual private networks (VPNs), Internet speed checkers, and graphics card software
- Logistics-themed cyber resources containing the string “parcel” and cybersquatting domains specifically targeting USPS

Our analysis of the artifacts’ web content also proved interesting. For example, this is the content of the legitimate Keepass website.

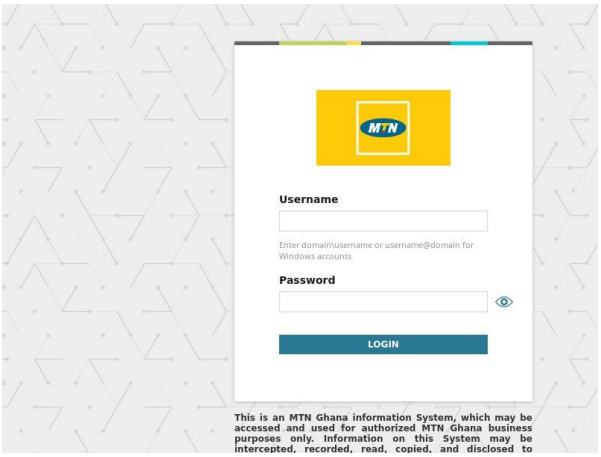


Meanwhile, the domain keepas[.]space hosted a look-alike page (at the time of writing).

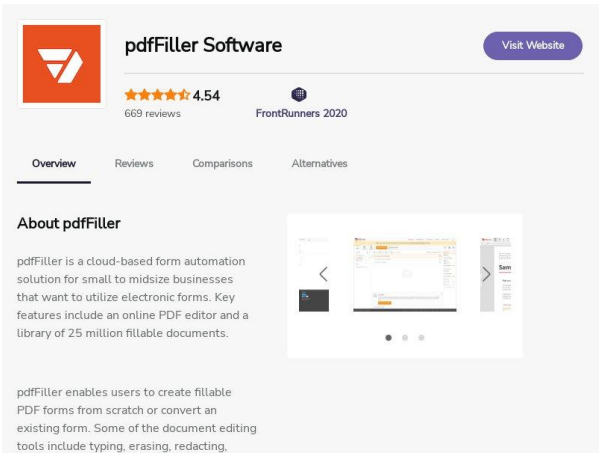
Other suspicious content hosted on the artifacts were consistent with those used in RomCom campaigns. Some of them are shown below.



Screenshot of pdfreader.digitalzone[.]today



Screenshot of npmsolarwinds01[.]mtn[.]com[.]gh

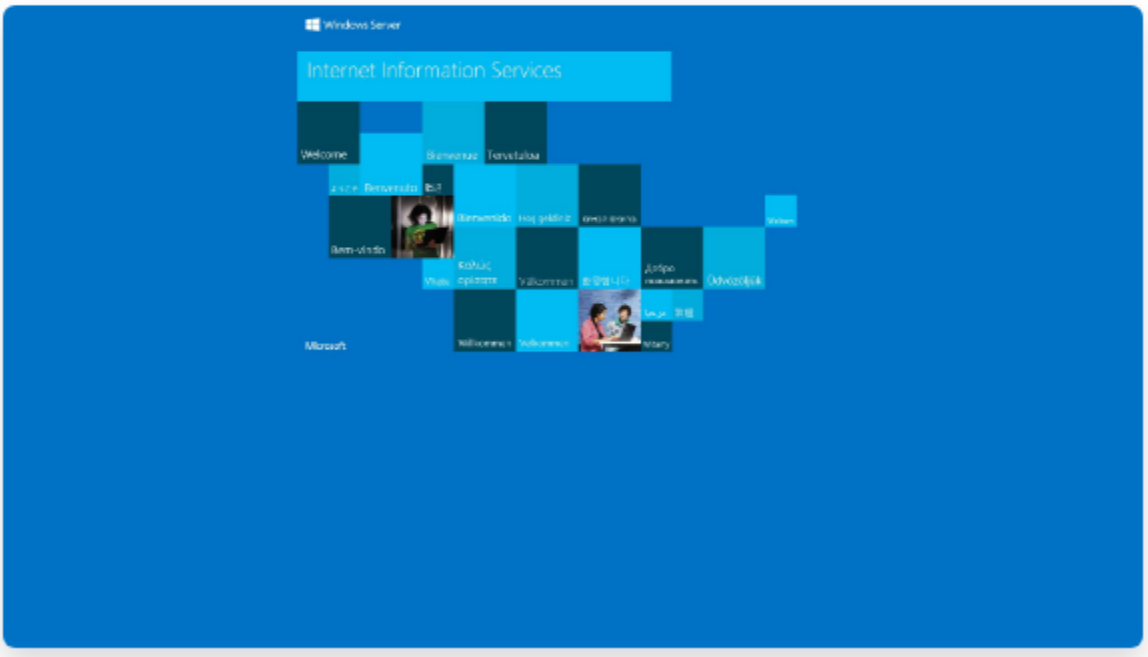


Screenshot of pdffiller-review[.]com

Screenshot of pdfreader[.]one

Several PDF Filler domains that have been flagged as malicious continued to host a Windows Server page like this.

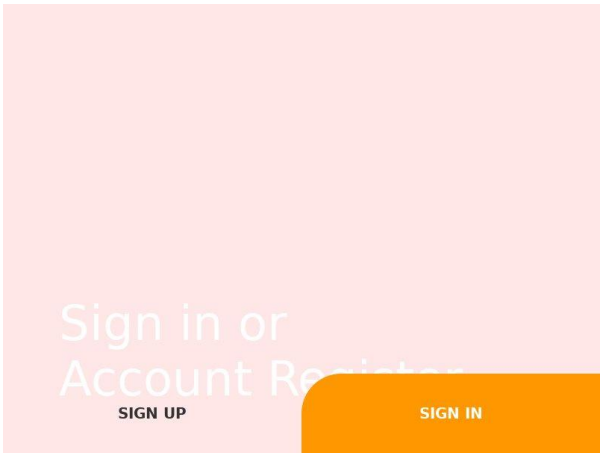
mail.pdffiller.x24hr.com website screenshot



Screenshot of mail[.]pdffiller[.]x24hr[.]com

Beyond RomCom

Various domains that host web pages bearing the SolarWinds logo and colors may indicate a broader campaign targeting the company. Here are some examples.



Screenshot of solarwinds-apps-sg[.]com

Screenshot of solarwinds-ranks[.]com

To recall, some of the malicious artifacts found seemed to target banks, logistics companies, and other products outside RomCom's known targets. These properties may belong to other threat actors. Regardless of the entities behind the suspicious artifacts, the damage they can incur remains the same.

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 Domains

Sample Public IoCs

- advanced-ip-scaner[.]com
- advanced-ip-scanners[.]com
- 167[.]71[.]175[.]165
- wveeam[.]com
- combinedResidency[.]org
- optasko[.]com
- 4qzm[.]com
- notfiled[.]com

Sample Artifacts Connected to RomCom

- 16059[.]noip2[.]net
- 163-mail-vertify[.]com
- 167-71-175-165[.]ipv4[.]nknlabs[.]io
- addr24[.]com
- advancd-ip-scanner[.]com
- advanced-ip-scanner[.]click

- advanced-ip-scanner[.]website
- advance-ip-scanner[.]website
- advncd-ip-scanner[.]com
- alqamegroup[.]net
- bedroomtoysdubai[.]net
- challengermodeaegis[.]net
- datamgmtveeamlenovo[.]com
- emusk2xe[.]com
- financeprotocol[.]net
- fraganciasluifesa[.]com
- gangstergo[.]com
- gospmr[.]net
- gpamf[.]net
- green1and-eg[.]com
- hl-1td[.]com
- investbtc[.]us
- keepaso[.]com
- keepass[.]space
- keepass[.]tech
- keepass[.]website
- keepasses[.]com
- keepassontomother[.]de
- keepassxc[.]website
- multipolar-veeam[.]com
- musk2xp[.]com
- myparcel-delivery[.]net
- myparcelusps[.]net
- myredeliveryusps[.]net
- my-uspsdelivery[.]net
- octoobay[.]com
- oneinchwalet[.]com
- oneinchwallet[.]com
- onlinebanking-scotiabank[.]com
- pancakeswp[.]com
- papafromgoa[.]com
- parlycrypto[.]com
- parlytrade[.]com
- pdffiller[.]business
- pdffillerofferad[.]shop
- pdffilleronline[.]com
- pdffillerr[.]com
- pdffillert[.]com
- pdfinfiller[.]com
- pdfreader[.]net[.]cn
- pdfreaderd[.]space
- pdfreaderdoc[.]space
- pdfreaderdocu[.]site
- perfumeriadistriaromas[.]com
- qamaraltaiy[.]net
- quilink1[.]com
- quilink2[.]com
- redelivery-myusps[.]net
- rotho-de[.]com
- scandic-iptv[.]com
- scan-ip[.]xyz
- secure-auth-gate[.]com
- secure-mail-login[.]com
- solarwind[.]press
- solarwindcars[.]eu
- solarwinds[.]au
- solpolas[.]com
- studyinbelarussia[.]net
- supporttpdffiller[.]com
- unifyerfound[.]net
- uniswap-claim[.]net
- updattee769cryy231capp[.]net
- usdms[.]us
- veeam[.]cpa
- veeam[.]cr
- veeam[.]sh[.]cn
- veeam01[.]ws
- veeamawscloudclique[.]com
- veeambrasil10anos[.]com[.]br
- veeamcloudconnect[.]africa
- veeamcloudconnect[.]durban
- veeamcloudrepository[.]com
- veeamcommunity[.]social
- veeam-jp[.]com
- veeamon[.]cn
- veeam-one[.]ws

- veeamonforummexico[.]com
- veeampaymentsolutionscert[.]com
- veeamransomwarequiz[.]com
- veeamtech[.]pl
- verlfy-pay[.]com
- www[.]media[.]combinedresidency[.]org
- www[.]search[.]combinedresidency[.]org
- www[.]wap[.]combinedresidency[.]org
- www[.]wiki[.]combinedresidency[.]org
- wwww[.]combinedresidency[.]org
- wyatt-barker[.]com
- zeus[.]combinedresidency[.]org
- zz[.]combinedresidency[.]org

Sample Properties Flagged as Malicious During the Malware Check Dated 18 November 2022

- advanced-ip-scaner[.]com[.]vuxuancuong[.]com
- pdffiller[.]x24hr[.]com
- www[.]pdffiller[.]x24hr[.]com
- mail[.]pdffiller[.]x24hr[.]com
- pdfreader[.]protocolfix[.]com
- pdfreader[.]ilhadoscaras[.]com[.]br
- www[.]pdfreader[.]ilhadoscaras[.]com[.]br
- www[.]pdfreader[.]protocolfix[.]com
- www[.]solarwindlv[.]askelsancho[.]com
- keepasses[.]com
- keepass[.]space
- keepass[.]website
- pdfreaderdo[.]space
- advanced-ip-scanners[.]com
- backstagecomms[.]com
- lomarter[.]com
- 14143[.]noip2[.]net
- 15310[.]noip2[.]net
- alfelahksa[.]com
- all4ocean[.]com
- allahwouakbaaahhh[.]co[.]in
- appprotonvpn[.]com