Detecting Malware Disguised as OneNote with Threat Intelligence

Table of Contents

Executive Report

We've seen threat actors abuse almost all Windows OS applications in their campaigns, disguising malware as macros, Word documents, Excel spreadsheets, and PowerPoint presentations to trick users into opening and executing them. Most recently, they've been spreading malware in the guise of OneNote documents to cause mayhem.

Threat Background

Proofpoint researchers Tommy Madjar, Corsin Camichel, Joe Wise, Selena Larson, and Chris Talib spotted threat actors distributing malware disguised as a OneNote document over the past 2–3 months. While some campaigns seemed to target specific industries in North America and Europe, thousands of emails with malware-laced OneNote document attachments have been seen infecting the computers of the general populace.

Email recipients tricked into opening and interacting with the supposed OneNote document attachment can end up with AsyncRAT, Redline, AgentTesla, DOUBLEBACK, or Qbot malware-infected computers. Possible effects include data stealing via credential theft and more.

The Proofpoint study identified 82 indicators of compromise (IoCs), including URLs, IP addresses, and SHA-256 hashes. We stripped some of them down, which left us with 17 domains and 13 IP addresses shown in the table below.

Domains	IP Addresses
• files[.]catbox[.]moe • onenotegem[.]com • transfer[.]sh	• 209[.]126[.]83[.]213 • 3[.]101[.]39[.]145 • 54[.]151[.]95[.]132

• depotejarat[.]ir • zaminkaran[.]ir • newtryex[.]ddns[.]net • stnicholaschurch[.]ca • winery[.]nsupdate[.]info • su1d[.]nerdpol[.]ovh • direct-trojan[.]com • mgcpakistan[.]com • plax[.]duckdns[.]org • ghcc[.]duckdns[.]org • barricks[.]org • kanaskanas[.]com • codezian[.]com • myvigyan[.]com	• 154[.]12[.]234[.]207 • 45[.]133[.]174[.]122 • 154[.]12[.]250[.]38 • 172[.]245[.]45[.]213 • 198[.]23[.]172[.]90 • 212[.]193[.]30[.]230 • 179[.]43[.]187[.]241 • 109[.]107[.]179[.]248 • 209[.]126[.]2[.]34 • 95[.]216[.]102[.]32

We used the IoCs as WHOIS and DNS tool search terms to scour the Web for other potential threat vectors through an in-depth IoC expansion analysis, which led to the discovery of:

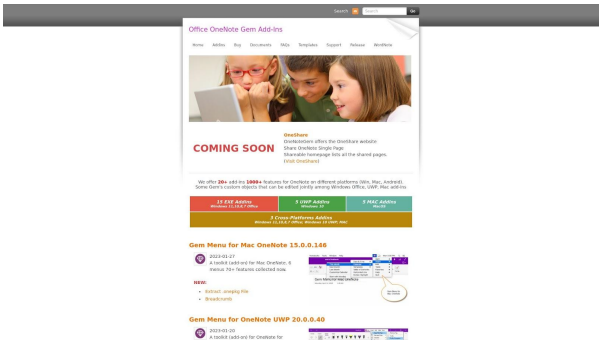
- Four unredacted registrant email addresses used to register an additional nine domains
- 11 IP addresses to which the domains resolved, four of which turned out to be malicious
- 1,992 IP-connected domains, 16 of which turned out to be malware hosts
- 32 string-connected domains

Unraveling WHOIS Ties

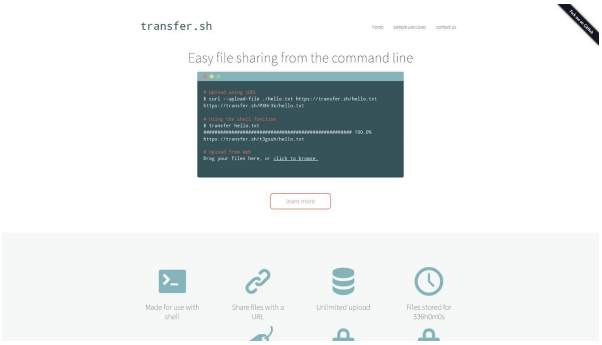
A look at the WHOIS records of the domains tagged as IoCs revealed the following findings:

- The oldest domain—mgcpakistan[.]com—was created on 8 June 2002 while the newest—direct-trojan[.]com—was created on 12 December 2022. A majority of the IoCs (80%) were aged domains.
- Six of the 17 domains—files[.]catbox[.]moe, onenotegem[.]com, transfer[.]sh, stnicholaschurch[.]ca, mgcpakistan[.]com, and codezian[.]com—continued to host live content with a few seeming to have been compromised legitimate sites for the threat actors' use based on their screenshots. Mgcpakistan[.]com, for instance, looks like the website of a legitimate medical equipment manufacturer.

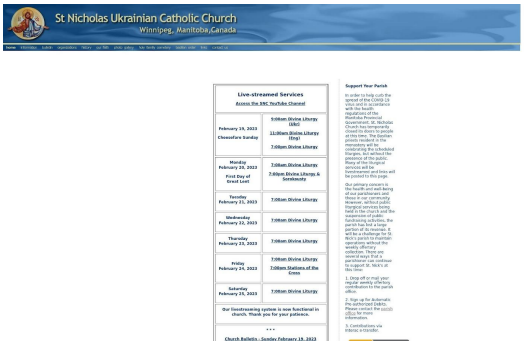
Screenshot of files[.]catbox[.]moe



Screenshot of onenotegem[.]com

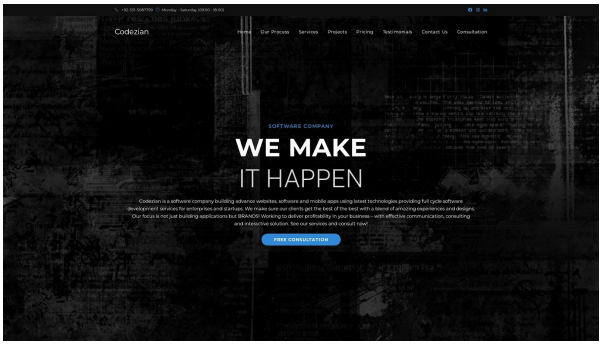


Screenshot of transfer[.]sh



Screenshot of stnicholaschurch[.]ca

Screenshot of mgcpakistan[.]com



Screenshot of codezian[.]com

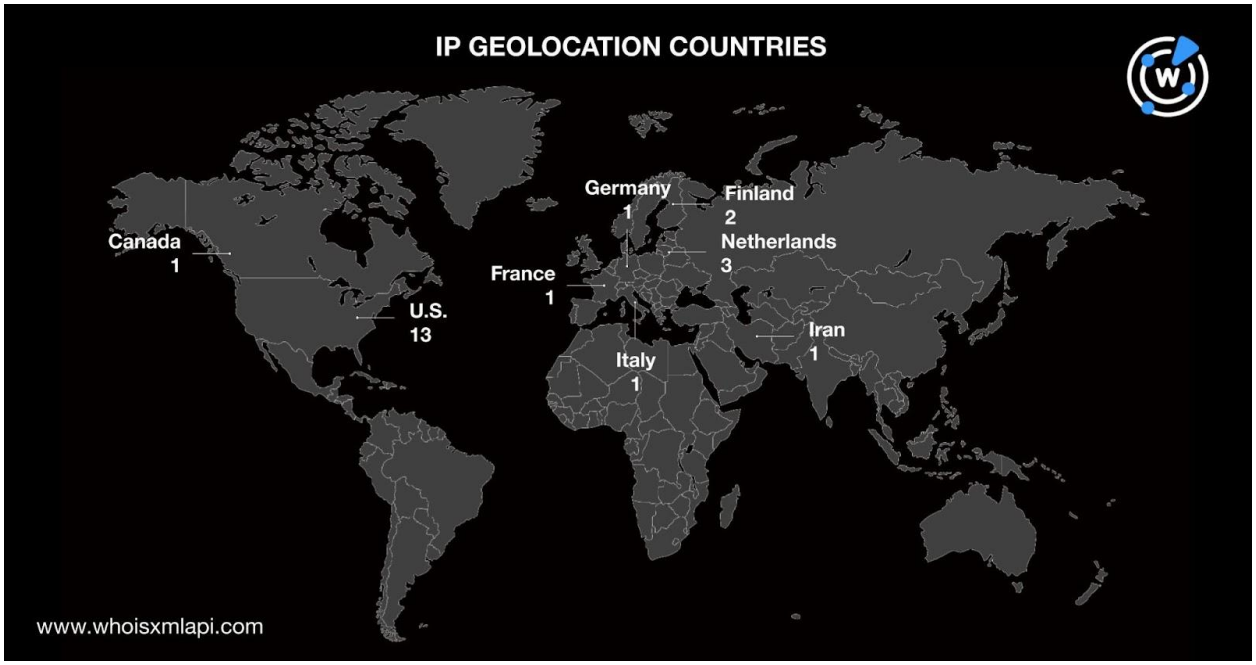
- The 12 domains with retrievable WHOIS records were spread across 10 registrars, primarily NameCheap, Inc.
- Four of the domains—onenotegem[.]com, depotejarat[.]ir, zaminkaran[.]ir, and barricks[.]org—had unredacted registrant email addresses in their historical WHOIS records. More interestingly, though, the email address used to register depotejarat[.]ir was also utilized for nine other domains, five of which are:

    - tejaratdepoo[.]ir
    - ariaevacuation[.]com
    - datisairconditioner[.]com
    - movieserial2[.]com
    - bardia-bardia[.]com

Under the DNS Lens

Next up, we looked at the IoCs through the DNS lens, which showed that the domains resolved to an additional 11 IP addresses that weren't included in the initial analysis's list. Four of these IP hosts turned out to be malicious, two of which are 107[.]160[.]74[.]134 and 95[.]216[.]33[.]194.

Like the first campaigns that targeted users in North America and Europe, 92% of the attack IP addresses were concentrated in the same continents. The map below shows the IP geolocation country breakdown of the 24 IP hosts.



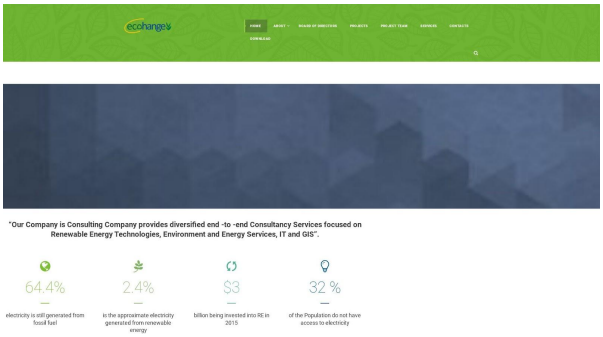
Reverse IP/DNS lookups for the IP addresses led to the discovery of 1,992 domains that shared the IoCs' hosts. A bulk malware check for these web properties revealed that 16 of them were malicious. Nine examples are:

- 2ndspreading1[.]ddns[.]net
- alphatradecapitals[.]com
- ariya-sanaat[.]ir
- ayot[.]ir
- beholdchk[.]com
- billionairedollarboys[.]com
- capitalglobetrust[.]com
- caricool[.]uk
- dronecammera[.]com

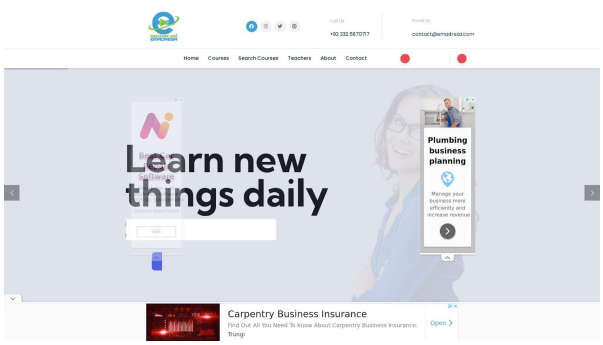
Despite being categorized as malware hosts, six of the domains continued to host live content.

Screenshot of capitalglobetrust[.]com

Screenshot of caricool[.]uk

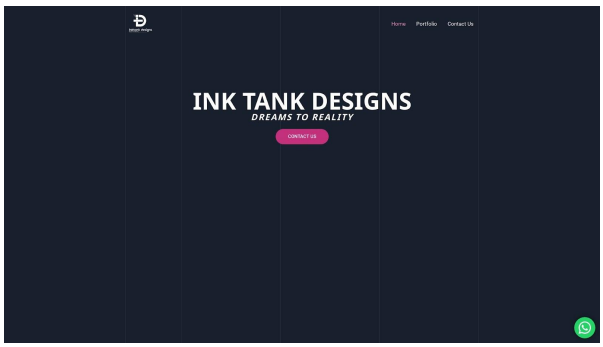


Screenshot of ecochange[.]com[.]pk



Screenshot of emadresa[.]com

Screenshot of fitsquadclothing[.]com



Screenshot of inktankdesigns[.]com

Some of the domains tagged as IoCs contained unique strings, including:

- ***zaminkaran.***
- ***depotejarat.***
- ***nerdpol.***
- ***direct-trojan.***
- ***barricks.***

Our searches on Domains & Subdomains Discovery found 32 additional domains that may be worth monitoring for signs of suspicious activity given their similarity with the IoCs.

—

Our deep dive into the malicious OneNote campaigns allowed us to identify 2,044 yet-unpublished artifacts, 24 of which have been dubbed malware hosts. The IoC expansion analysis results could be useful in early threat identification and mitigation for organizations.

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 Email-Connected Domains

- tejaratdepoo[.]ir
- ariaevacuation[.]com
- datisairconditioner[.]com
- movieserial2[.]com
- bardia-bardia[.]com

Sample IP Address Resolutions

- 107[.]160[.]74[.]134
- 107[.]173[.]157[.]123
- 144[.]76[.]136[.]153
- 95[.]216[.]33[.]194
- 185[.]81[.]96[.]5
- 69[.]27[.]118[.]3

Sample IP-Connected Domains

- a-to-b-sedan[.]com
- a1generate[.]com
- a3[.]6mail6[.]xyz
- a31[.]6mail6[.]xyz
- a34[.]6mail6[.]xyz
- a35[.]6mail6[.]xyz
- a36[.]6mail6[.]xyz
- a37[.]6mail6[.]xyz
- a38[.]6mail6[.]xyz
- a40[.]6mail6[.]xyz
- a44[.]6mail6[.]xyz
- a5[.]6mail6[.]xyz
- a7[.]6mail6[.]xyz
- a9[.]6mail6[.]xyz
- aa[.]indushosters[.]com
- aajees[.]com
- aarushfoundation[.]co
- aasco[.]pk
- abanplus[.]com
- abanplus[.]ir
- abbasi-trading[.]ir
- abc123[.]doctorhoster[.]com
- abdolsalam1401[.]ir
- abdullahqurantutor[.]com
- abhavijbastani[.]ir
- abhavijbastani[.]pofaknamaki[.]ir
- abhinav[.]cucampus[.]in
- abidartaps[.]com
- abidartaps[.]ir
- aboatashsafetyco[.]com
- abossmove[.]com
- abreec[.]com[.]pk
- abtin-trm[.]ir
- abzarpasand[.]com

- abzarpasand[.]ir
- academybartar[.]ir
- academyewebsite[.]ir
- academyheydarnia[.]ir
- account[.]suite300[.]co
- accountaxlive[.]com
- accounts[.]ladprocrypto[.]com
- ace-webapp[.]com
- acerhoster[.]com
- achbakh[.]ir
- acornstairlifts[.]ir
- acsbmd[.]org
- activefricensured[.]com
- actoractressacademy[.]com
- adabraillesupply[.]com
- adaklab[.]ir
- adammeeker[.]com
- adarchstudio[.]com
- adatheme[.]ir
- addleven[.]com
- addlevenpharma[.]com
- addrace[.]com
- addvcash[.]com
- adera[.]pk
- adinstruments[.]ir
- adlemobin[.]ir
- adlinker[.]org
- adorg[.]net
- adrianzator[.]com
- adrintinboxorg[.]com
- adroitcollaboratives[.]com
- adscornerblogs[.]com
- adshelp[.]ir
- advancedit[.]ir
- advari24[.]ir
- aeinnovationsgroup[.]com
- afewgoodmoods[.]com
- affiliatestore[.]pk
- afmarketing[.]com[.]pk
- afomods[.]org
- afourstarweb[.]com
- africanbitterleaf[.]com
- africansocialnet[.]com
- afsanehyogaclub[.]ir
- aftabkaroon[.]ir
- aftertech[.]ir
- afzaleconomist[.]pk
- agamslot[.]com
- agencialfr[.]com
- agentcity-pk[.]com
- aghamiriskincare[.]com
- agnosticworld[.]info
- agricultureajk[.]org
- agrotop[.]ir
- agslot2[.]com
- ahan-iron[.]com
- ahan-iron[.]ir
- ahankadepanahi[.]ir
- ahglobal[.]com[.]pk
- ahjam[.]ir
- ahmadnazari[.]ir
- ahouraparsian[.]com
- ahouravira[.]ir
- ahvazdog[.]com
- ahvazmarket[.]com
- ahvazyab[.]com

Sample Malicious IP-Connected Domains

- 2ndspreading1[.]ddns[.]net
- alphatradecapitals[.]com
- ariya-sanaat[.]ir
- ayot[.]ir
- beholdchk[.]com
- billionairedollarboys[.]com
- capitalglobetrust[.]com
- caricool[.]uk
- dronecammera[.]com

Sample String-Connected Domains

- onenotegem[.]net
- onenotegem[.]cn
- depotejarat[.]com
- zaminkaran[.]com
- nerdpol[.]fm
- nerdpol[.]garden
- nerdpol[.]media
- nerdpol[.]org
- nerdpol[.]eu
- nerdpol[.]io
- nerdpol[.]co
- nerdpol[.]info
- nerdpol[.]estate
- nerdpol[.]rocks
- nerdpol[.]com
- nerdpol[.]tk
- nerdpol[.]it