

## Holiday Bazar: Tracking a TrickBot-Related Ransomware Incident - DomainTools | Start Here. Know Now.

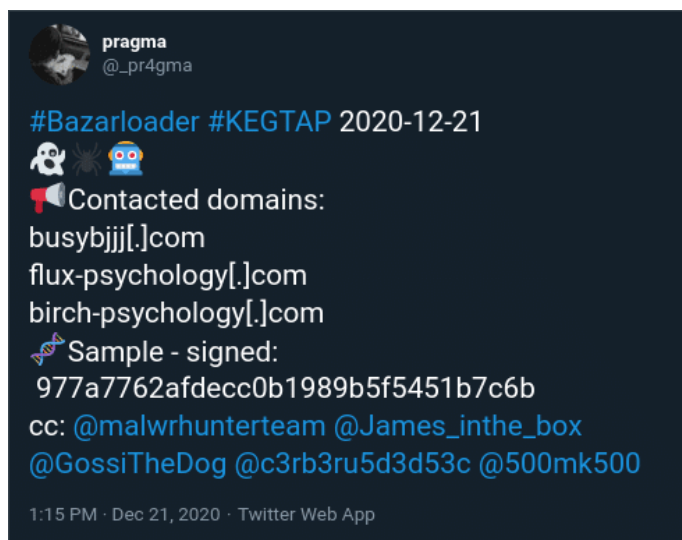
By Joe Slowik

Published: 2021-01-06 · Archived: 2026-04-05 23:36:01 UTC



### Background

On 21 December 2020, the start of the Christmas week, evidence emerged of a ransomware campaign leveraging [BazarLoader](#) (also referred to as [KEGTAP](#)) and linked to the [TrickBot](#) ransomware gang. Initially disclosed in a tweet, the campaign rapidly unfolded over the course of that day.



Based on discussions with intelligence partners and various network defenders, the adversaries responsible for this activity appeared to rapidly move from initial infection at victim locations to interactive operations en route to attempted ransomware deployment. In previous operations, TrickBot activity is associated with the [deployment](#) of [Ryuk ransomware](#). At the time of this writing, DomainTools researchers were unable to confirm a final-stage payload for this specific campaign.

Although this specific campaign has since passed, it contains many lessons for network defenders and Cyber Threat Intelligence (CTI) professionals for monitoring and analyzing emerging campaigns to enable dynamic, flexible defense.

### Initial Delivery and Download Vector

Analysis of the campaign indicates initial delivery takes place using a legitimate third-party email messaging or notification service. In this specific case, the adversary leveraged [GreatResponse](#), used for email marketing and landing page design, to deliver seemingly benign-looking email messages with “Corporate Document” or similar themes. Observed link examples include the following:

```
corpdocument1221.gr8[.]com  
companygeneralmeeting122220.gr8[.]com  
Companydocument07851-3173f.gr8[.]com
```

When accessed, a victim would see a landing page such as the following:

## STATEMENT [#5937](#)



[SAVE AND PREVIEW](#)

According to the company rules this document is available only on corporate computers. If it doesn't start automatically, [click here](#).

The link would direct to a Portable Executable (PE) file, discussed in further detail below, hosted on Google Drive. Further execution would require the user to run the downloaded executable for follow-on exploitation to occur.

The above activity is consistent with observed TrickBot operations—as well as other entity tactics—using third-party services to evade detection and mitigation. For example, TrickBot gang campaigns have previously used [third-party delivery services](#) such as [Sendgrid](#) to distribute initial phishing messages. Follow-on payloads have also been hosted on cloud file storage sites, such as [Google Drive](#), as well.

### Examining Droppers and Installers

Further activity requires not only user interaction with the phishing message (displaying the landing page link) and downloading the file hosted from Google Drive, but then executing the payload as well.

Overall, as part of the completion of this “kill chain,” DomainTools researchers observed 18 samples of the next-stage payload. Naming conventions for these files matched the landing page themes, although DomainTools researchers expect more variants likely exist beyond our visibility.

| SHA256   | MD5                              | File Name         |
|--|----------------------------------|-------------------|
| 90a51557f3438fec9b2ffab5828751cb43fa9eeb1fa84468effe95a9f13f12d0 | 774bdb15ae6c7dedea62ebf0985a3451 | Corp_Document.exe |
| 74d757a4cabf26009ab5f1064939c54ceea43a8399419a7c965b2edb7e0ed648 | 2d8c8177ab8ddb90a42ea03827eeb37  | Company_Doc.exe   |
| 0e809ef68d85e730190db2663ab914dfd6ccb4c355a051841366b3a5c91ada63 | 0dd55da99e569959b4a338c5ef67e2b4 | Corp_pdf.exe      |
| 2be628add2ab1be6120026893c6a7a51dc0b3f81c7421349504a6010581aa427 | a54c10b1372f0dcc492d78349d7d2ad4 | Corp_Document.exe |
| 21df8a331f272ed9b6b72509028af31612292c9f3c0776a4472b2b585c142648 | eeb42010fcbabf4079994a831637105f | Company_Doc.exe   |
| 82dbcaa7694a6e763300cee1d4b2ef6e65f6a65fd93663365ce032823984cb21 | 7ef4f4eb66ea52a0f1471169e2a53758 | Corp_Document.exe |

| SHA256  | MD5                              | File Name         |
|---|----------------------------------|-------------------|
| 2c6b49185dea80c48dcdd1c316a0de3413ff52a67819a720419c630093b5e638  | 1cd5e8bbd17c4764f9db10529bd25608 | Company_Doc.exe   |
| 3941242436e943fbfb7b1767aa2615bcc5637da3d939d3b06a1572de8bf044a1  | 5af82b394bae65462bfb643933c09930 | Doc_21.12.exe     |
| 4c4b00621d0e57bcdff188174a539ca3c92a4fc96647eabe6d79c17ae04bd519d | f0cc16198bdf3ef628264794bf074817 | Corp_pdf.exe      |
| 3985648d781de545cf1209469454b88f7f6e54696b6a050dbb7ba2ba1eae2cec  | c3ad311ea64ad7981b6451f47ff88202 | Corp_Document.exe |
| 436301cb89dadedcb6c6cfc043b8a4d8f47de2054b1e84e1612cf061cd14dc15  | 977a7762afdecc0b1989b5f5451b7c6b | Company_Doc.exe   |
| 44075e5eb7ee76b006a8f4cf2bfee30dec3c5007c02f8657f956429bb976ea4b  | d52710baa7cc837a628a5ef1c5cdfd92 | Doc_21.12.exe     |
| bed288ad6037546ecfb9e912518583fefbb7685681a8ecfd5b27502735de20bd  | b0c831758a9726010f13058e37c7c2c5 | Corp_Document.exe |
| 102dca8d268dbbba33770459009d4d67e0d714b44523c28fce57ee83fe186a31  | e018926f81bf4599dedb4ae1696689b1 | Corp_pdf.exe      |
| bbe896ab541c703d699f97311a30c2e07be98be1ebf7eed9a9a1fd7dfa2efb5b  | de65816eca59774ffc2fa96cebc68c8  | N/A               |
| 69aa97d3507d4ccf7dc0bd0a97cfe509edfbd16734fcc40cd01d8dd659fd450   | 4c52e80e6bb5452f42600ee7bb5c4ee7 | View Report.exe   |
| 392c73ffa3b1513cd8de9435d7e76320eff7f98db884eb6bc776c3b2bea7c77e  | eea12082de2cbb26af85b4060c4baa34 | Corp_Document.exe |
| e1841e78c6dace694cc5172bac1068b9ede38a3623c5429a877eb1190d90a14d  | bd7d9ae98ec2adf3c9e545b9567a4b8c | Company_Doc.exe   |

One sample, "View Report.exe", is a 32bit executable that appears to date from late November 2020 and from part of an earlier, undocumented campaign. The remaining samples are 64bit executables compiled on the day of the campaign, 21 December 2020.

The executables in this campaign are signed with the same Sectigo code signing certificate, with the name "СКАРАБЕЙ" (Russian for "Scarab") and a fingerprint value of "348F7E395C77E29C1E17EF9D9BD24481657C7AE7." This certificate has since been revoked by the issuer.

**Signers**

— ООО "СКАРАБЕЙ"

|               |  |
|---------------|--|
| Name          | ООО "СКАРАБЕЙ"   |
| Status        | Trust for this certificate or one of the certificates in the certificate chain has been revoked. |
| Issuer        | COMODO RSA Extended Validation Code Signing CA   |
| Valid From    | 12:00 AM 11/04/2020  |
| Valid To      | 11:59 PM 11/04/2021  |
| Valid Usage   | Code Signing   |
| Algorithm     | sha256RSA  |
| Thumbprint    | 348F7E395C77E29C1E17EF9D9BD24481657C7AE7   |
| Serial Number | 23 4B F4 EF 89 2D F3 07 37 36 38 01 4B 35 AB 37  |

While signed binaries [are not new](#) to ransomware or related operations (with notable signed examples including but not exclusive to [Ryuk](#) and [LockerGoga](#) variants), they continue to pose a threat to users as many applications and security products inherently trust code-signed items.

Following successful binary execution (through user interaction), the malware attempts to resolve and connect to one of at most two Command and Control (C2) servers embedded within the binary. Successful connectivity allows for further actions on target, including the attacker taking control of implants to launch further commands or move laterally within the victim environment.

**Associated Network Infrastructure**

As noted in the original Tweet sparking this investigation, there were several domains immediately identified as associated with this campaign. Further investigation and analysis of samples yielded additional items, shown in the following table:

| Domain                 | Registrar     | Create Date | IP              | Hosting Provider | SSL Certificate Hash                  |
|------------------------|---------------|-------------|-----------------|------------------|---------------------------------------|
| birch-psychology[.]com | NAMECHEAP INC | 12/10/2020  | 192.236.155.212 | Hostwinds LLC.   | 2929ea338eb1a9aeb83aa8dcf08148125059f |
| busybjjj[.]com         | NAMECHEAP INC | 12/10/2020  | 195.123.241.79  | ITL-Bulgaria     | 5a8da3e012eee5505a04e09a1e323acbb1c14 |

| Domain                     | Registrar     | Create Date | IP              | Hosting Provider  | SSL Certificate Hash                  |
|----------------------------|---------------|-------------|-----------------|-------------------|---------------------------------------|
|                            |               |             |                 | Ltd.              |                                       |
| flourish-psychology[.]net  | NAMECHEAP INC | 12/10/2020  | 192.119.171.165 | Madgenius         | b93e985da0cc7d540c4ebddf9136dbf948e7? |
| flux-psychology[.]com      | NAMECHEAP INC | 12/10/2020  | 107.152.32.121  | ServerCheap INC   | 4ee5e1eaaab74ccb04010b735b75d5b3b98a  |
| freekarateel[.]com         | NAMECHEAP INC | 12/10/2020  | 94.140.114.152  | SIA Nano IT       | dbd1959d1a0575219f265ed48bfe71ca4225- |
| impactpsychcoloradoo[.]com | NAMECHEAP INC | 12/10/2020  | 185.82.127.115  | SIA Nano IT       | 2852cb1c32b90554e5fd2b6b8e494c45d1e6  |
| livingyoga-denver[.]com    | NAMECHEAP INC | 12/10/2020  | 138.201.113.2   | Hetzner Online AG | 52b825408a1cb843e84d623e6506c29e807e  |
| ustfitf[.]com              | NAMECHEAP INC | 12/10/2020  | 195.123.240.192 | ITL-Bulgaria Ltd. | e5add3d65ebeba577d383657148f92fd53f3? |

The identified network infrastructure serves as the next stage of the intrusion. Following malware installation, active C2 would be used to further exploitation of the victim, leading to likely ransomware activity.

### Pivoting and Identifying Additional Items

At this stage, we as defenders are largely in a “reactive” state with respect to identifying indicators and characteristics of this BazarLoader campaign. While quickly ingesting and deploying defensive measures based on indicators and observables may represent an improvement over completely passive defense, it still leaves much to be desired.

Instead, by identifying characteristics inherent to the campaign—both its network infrastructure and malware samples—we can both gain greater knowledge of the attacker’s tendencies while enabling defense attuned to these tendencies. For the latter, this means adapting defense to the adversary’s fundamental behaviors as opposed to chasing specific examples of those behaviors as represented by indicators.

### Network Observables

Looking at the domains identified above, several “themes” emerge:

- Typical use of naming “themes” reflecting local service providers or small business entities, with an emphasis on “cleaning” companies.
- Consistent use of NameCheap for registration purposes.
- Almost exclusive use of the “.com” Top Level Domain (TLD).
- Creation on the same day, 10 December 2020.
- Hosting on various relatively small, privacy-focused Virtual Private Server (VPS) providers.
- Use of Let’s Encrypt SSL certificates for encrypted communications.

As [previously documented by DomainTools](#), these observations can be used to unearth additional C2 infrastructure for threat hunting or preemptive defensive purposes. Unfortunately, at first glance by plotting the above items using DomainTools Iris visualizations, there seems little in common on a technical level to enable successful pivoting to additional infrastructure.



Yet a combination of limited technical details that overlap (registrar, TLD use, and time of creation) along with “thematic” observables (the naming conventions used) can enable us to unearth additional items.

With this hypothesis in mind, looking for items with a similar technical structure that also mirror the “local service” or “local business” theme, we can identify the following through DomainTools Iris:

| Domain                        | Create Date | IP              | ISP                           | SSL Certificate Hash                     |
|-------------------------------|-------------|-----------------|-------------------------------|--|
| app-space-cleaner[.]com       | 12/15/2020  | 46.4.76.174     | Hetzner Online AG             | d456b68598481ca23f7736828731c3730d641192 |
| babynamesinspirations[.]com   | 12/14/2020  | 135.181.154.50  | Hetzner Online AG             | N/A                                      |
| bbdworld[.]net                | 12/18/2020  | 195.201.9.204   | Hetzner Online AG             | N/A                                      |
| blacksockproductions[.]com    | 12/10/2020  | 192.119.162.84  | Madgenius                     | N/A                                      |
| blueridgecabin-cleaning[.]com | 11/13/2020  | 94.140.115.253  | SIA Nano IT                   | 5392b3c24963f7de3c3f7e0711d4f6eba4f0f31a |
| carwashevanstoon[.]com        | 12/15/2020  | 94.140.114.54   | SIA Nano IT                   | a856e01b468b46f4316ef026bf74351ce27647c5 |
| cgschool[.]com                | 12/9/2020   | 116.203.253.24  | Hetzner Online AG             | N/A                                      |
| cleaningcompany-online[.]com  | 12/1/2020   | 192.227.231.237 | Virtual Machine Solutions LLC | 1eab0efacfeb82bde18db1200ff03bb0526ac60d |
| coloradobudokann[.]com        | 12/10/2020  | 195.123.233.78  | ITL-Bulgaria Ltd.             | N/A                                      |
| crowleycollegeprepp[.]com     | 12/10/2020  | 107.152.42.146  | ServerCheap INC               | N/A                                      |

| Domain                      | Create Date | IP              | ISP                 | SSL Certificate Hash                     |
|-----------------------------|-------------|-----------------|---------------------|--|
| data1-posten[.]com          | 12/7/2020   | 168.119.171.234 | Hetzner Online AG   | 30f46401c6abd0c9a629c64259592b5c6ca974a6 |
| familyzstore[.]com          | 12/11/2020  | 198.54.117.244  | Namecheap Inc.      | N/A                                      |
| first-posten[.]com          | 12/7/2020   | 168.119.171.234 | Hetzner Online AG   | N/A                                      |
| form-feedback[.]com         | 12/7/2020   | 178.63.220.179  | Hetzner Online AG   | 23f3a3a27edcb956c33aa57c71abcd34e6c454c  |
| greatsfamily[.]com          | 12/9/2020   | 198.54.117.244  | Namecheap Inc.      | N/A                                      |
| injektorrx[.]com            | 11/13/2020  | 94.140.114.187  | SIA Nano IT         | 0aec5a4f8860b44d77fb47f053e391c83aa36cfb |
| inmanheatingandcoolng[.]com | 12/15/2020  | 94.140.114.135  | SIA Nano IT         | 66688b898713f2d840985325d093e46e5fbbc0e6 |
| intlupdate[.]com            | 12/8/2020   | 5.34.178.204    | ITL LLC             | 35d8a65cba2c02c4dcc7bb7e00680ae5c4aa4823 |
| johnnyclean-carwash[.]com   | 12/1/2020   | 192.119.171.231 | Madgenius           | a24abeb13e6ad93f9c82af26352d33a358c9c634 |
| johnnykashjewelsapp[.]com   | 12/15/2020  | 195.123.237.139 | ITL- Bulgaria Ltd.  | N/A                                      |
| jordanbelforthiring[.]com   | 12/16/2020  | 192.64.119.2    | Namecheap Inc.      | N/A                                      |
| kizenservices[.]com         | 12/9/2020   | 195.201.179.80  | HostMaster Corp     | N/A                                      |
| lovelyhomemart[.]com        | 12/7/2020   | 176.9.29.52     | Hetzner Online AG   | 9b48c3e61c1aa79155b725f5fd4f47bc755d0d2d |
| manageupdatenetwork[.]com   | 12/17/2020  | 94.140.114.160  | SIA Nano IT         | N/A                                      |
| my-space-cleaner[.]com      | 12/10/2020  | 46.4.76.174     | Hetzner Online AG   | b613424256682a4a4d4465a8b84741e4055f211b |
| newappday[.]net             | 12/9/2020   | 95.217.229.116  | Hetzner Online GmbH | N/A                                      |
| niftythriftsteals[.]com     | 12/13/2020  | 49.12.15.63     | Hetzner Online AG   | 630a232a25964fbd8031ecfd5860c7578210222  |
| nord-city[.]com             | 12/11/2020  | 46.4.70.54      | Hetzner Online AG   | 179e434d8e2b4c6190037f55bf94c1c766e58777 |
| open-register[.]com         | 12/16/2020  | 198.54.117.197  | Namecheap Inc.      | N/A                                      |
| posten-order[.]com          | 12/7/2020   | 168.119.171.234 | Hetzner Online AG   | a6c19e7d55629da02919432bd5e92bd8395715e7 |
| pulsehomeowner[.]com        | 12/14/2020  | 159.69.186.9    | Hetzner Online AG   | N/A                                      |
| qureshisgym[.]com           | 12/20/2020  | 95.216.159.168  | Hetzner Online GmbH | N/A                                      |
| real-posten[.]com           | 12/9/2020   | 135.181.94.39   | Hetzner Online AG   | N/A                                      |

| Domain                     | Create Date | IP              | ISP               | SSL Certificate Hash                     |
|----------------------------|-------------|-----------------|-------------------|--|
| rentinginnovations[.]com   | 12/13/2020  | 159.69.186.9    | Hetzner Online AG | N/A                                      |
| rmflaging[.]com            | 12/10/2020  | 94.140.115.145  | SIA Nano IT       | N/A                                      |
| service-masterss[.]com     | 11/13/2020  | 141.136.0.3     | SIA Nano IT       | N/A                                      |
| speed-posten[.]com         | 12/11/2020  | 135.181.94.39   | Hetzner Online AG | N/A                                      |
| stonyhand-carwash[.]com    | 12/15/2020  | 138.201.112.173 | Hetzner Online AG | N/A                                      |
| tracking-posten[.]com      | 12/7/2020   | 168.119.171.234 | Hetzner Online AG | b62aed1d366c54148617c3c30f6883b0a92c4aa6 |
| trak-no-posten[.]com       | 12/10/2020  | 135.181.94.39   | Hetzner Online AG | N/A                                      |
| trakaing-pass-posten[.]com | 12/9/2020   | 168.119.171.234 | Hetzner Online AG | 1fac7b2ae6b7ea5b7c032c9cd1f06db9844a6a72 |
| washguystxx[.]com          | 12/4/2020   | 141.136.0.25    | SIA Nano IT       | N/A                                      |
| worldnewsfeed[.]net        | 12/15/2020  | 88.99.102.85    | Hetzner Online AG | f852a683482e9fbab0044e0257eee159e0bdf044 |

This list is extensive and includes items that are likely not related to this campaign, but other items seem to fit the pattern observed quite well. Examples include:

```
blueridgecabin-cleaning[.]com
carwashevanston[.]com
cleaningcompany-online[.]com
coloradobudokann[.]com
Johnnyclean-carwash[.]com
stonyhand-carwash[.]com
```

These items form the basis for further threat hunting and CTI analysis. Given that all of the identified items are marked as likely malicious based on DomainTools risk scoring algorithms, the options available to defenders range from adding the domains and related infrastructure to blocklists as a preventative measure to monitoring them for further activity. For example, items such as those called out above could be flagged in various services, such as DomainTools domain monitoring, to identify when changes or file associations occur.

### File Patterns

In addition to domain patterns, the malware samples associated with this campaign also feature several commonalities that can be used for either hunting or alerting purposes, depending on the tools and visibility available to the researcher. From the information available thus far, we have the following insights:

- Exclusive use of 64bit binaries downloaded from cloud storage providers.
- Use of the same Sectigo signing certificate across all known samples.
- Common file naming conventions based on variations of “company report” and similar themes.
- Commonality in C2 infrastructure.

From the above, DomainTools researchers began investigating multiple data sources for similar file characteristics as well as items contacting domains revealed in the network pivoting exercise documented in the previous section. From this and follow-on analysis from initial findings, DomainTools researchers unearthed another BazarLoader campaign from 17-18 December 2020. The following samples and C2 domains were observed:

| SHA256   | MD5                              | File Name | C       |
|--|----------------------------------|-----------|---------|
| b455c245254ebf9691dcf7f02323b42c5b34998a440fa1b8a0f981f0ce3e2bfb | f1672efcf0685d933fe104e1c4639a64 | N/A       | jc<br>c |

| SHA256   | MD5                              | File Name        | C                           |
|--|----------------------------------|------------------|-----------------------------|
| c9a66cff4c5b5d74545c1eabc9da4ecf618f9c72174150569daa58e843cee5e5 | c28b472f5162a4a58d29aed1f1b2fe06 | BonusReport.exe  | jc<br>c<br>a<br>l<br>s<br>t |
| a7738dddb62919658c1fe3d339ccae6d0d2afe85a1bccccfce6f8a9ee6b4c5de | 356bc937d6e70bbc75ed7a3c47a2f184 | AnnualDoc.exe    | cl<br>o                     |
| 0d848d9675e6e6d12d1d158b07b636db246e02145beb5db7ae9be36cb5e1c3ff | 872608fe080163292505b2bc5e8880c0 | AnnualDoc.exe    | jc<br>c                     |
| 68ed893ae6ab2d7f00c3aacf46bc0c92966b647bcfe7e940a5d3ee55af01105a | 3ec43f75ab39833054610e3e6f0cb217 | AnnualDoc.exe    | jc<br>c                     |
| c67c3cc34905f4751e2f48363a0cf3cf69799f020687b6f5852058d3abd1c31d | a13275cb285c392c9ddc765d0f5f0754 | BonusReport.exe  | jc<br>c                     |
| 7978e198f7523d487e13a742101810d765c4ed191920d571ea51c99cc18eb795 | 8763f3f259a7f7fb8e9e91cd3d6491c7 | N/A              | jc<br>c                     |
| d33a8c70a8ae4f8eeb2f3708820486c0248edf340120f6380a8a3540e212a5dc | 946c9c2574feaca8d674914faeeca65a | BonusReport.exe  | jc<br>c                     |
| 9b29924a22ef01cb9c3b8c98d5cc4508836427335d3949c93e7a4c50c2bd40d5 | 9014ee7a206b40f1cf81de0918ff8c9f | AnnualReport.exe | cl<br>o<br>a<br>l<br>s<br>t |
| 75a52886c5a83dd25cb7e7d393320ee439f7605dbe41818057fc34c1102bbfc1 | b8648e857b5e80920bd08a749b3d57ba | AnnualDoc.exe    | cl<br>o                     |
| bcccb14658e8c1bee8107a2c314957c2bd9e505e73012b0aaa18df9fedf99248 | dd0c5c4d2cdf6f57be6c7f4d7e64f5fd | AnnualReport.exe | jc<br>c<br>r                |
| 56c5bee33c17a453c900725f88efb0466fd928072c420955fa599b518b9dfcd2 | ee85e8c0956d2021732d9606120401f9 | AnnualReport.exe | cl<br>o<br>a<br>l<br>s<br>t |
| 898f6e91c82bf23b5b95e0560292b1c610970b3062eeeb9980c75f954e5024a9 | 2946562b29462362faf215bf7a2fcaa6 | BonusReport.exe  | jc<br>c                     |
| 7ed66b0d81958d709b7f3067f9bdc69c25cbb955506c4a812cf0b6b9a7590f0d | 949099803fcee51754b88ad6d121fb46 | AnnualDoc.exe    | jc<br>c                     |
| a32ed4b36d44c489341721920d27294cab78ad7bd970c8ac6baa3edc4337a600 | 5686d8ae3dbaf2898116583c91adf368 | BonusReport.exe  | h<br>h                      |
| 288d28f4d53d8e44d599a4d2f70b53d5b13f0827ad2b7a953a7a3cbd6e67bf25 | dfa0bc9da86deb5f9419d96d5dc60a64 | N/A              | jc<br>c                     |
| ac696ef5a12039b72e408b6b14e08823c407ee652a6a36b7c33d01cd8d373497 | 67c2474a2fb201491c0ff5ff7ab783ea | AnnualReport.exe | jc<br>c<br>a<br>l<br>s<br>t |
| 30b2922c78a07dcd65af93886e7efcd6c3c883c70c2dc5f37cf41e50f240903  | f7079cd6f7bb70b8a341af27c62be1aa | AnnualReport.exe | jc<br>c                     |

Multiple samples were identified with C2 infrastructure linked to the domain pivoting in the previous section. While this did not appear to succeed in identifying “new” items (as the files in question appear to have been active from 17-18 December 2020, before the originating campaign sparking this investigation), their discovery indicates other items in the list of possible domains may relate to future campaigns by the same actor. Additionally, some items were revealed which featured C2 domains not related to the pivoting documented earlier. Examples include:

```
akbuilding-services[.]com  
Homeclean-heroes[.]com  
Maidtoorderfl[.]com
```

Although exhibiting C2 domains beyond initial research, the items were linked by a common code signing certificate (again from Sectigo, and since revoked by the issuer) with the name “ИНТЕЛЛИТ” (Belorussian for “Intelligence”) and thumbprint “1103DEBCB1E48F7DDA9CEC4211C0A7A9C1764252”:

Signers

- ООО "ИНТЕЛЛИТ"

|               |  |
|---------------|--|
| Name          | ООО "ИНТЕЛЛИТ"   |
| Status        | Trust for this certificate or one of the certificates in the certificate chain has been revoked. |
| Issuer        | COMODO RSA Extended Validation Code Signing CA   |
| Valid From    | 12:00 AM 12/01/2020  |
| Valid To      | 11:59 PM 12/01/2021  |
| Valid Usage   | Code Signing   |
| Algorithm     | sha256RSA  |
| Thumbprint    | 1103DEBCB1E48F7DDA9CEC4211C0A7A9C1764252   |
| Serial Number | 77 89 06 D4 06 95 F6 5B A5 18 DB 76 0D F4 4C D3  |

Although a different certificate than that used in the 21 December campaign, it reflects similar themes and observations. One item in common with both signing certificates is the prefix “ООО”, which in Russian (and related) languages is equivalent to “Ltd.” While there are many legitimate entities that can and do sign their software with certificates including “ООО” in their name, this may function as a robust indicator for organizations with few or no commercial ties to Russian or related language entities for blocking or filtering files with code signing certificates containing such language. This code signing observation represents a start in overall defensive planning against malware campaigns such as that observed in this report.

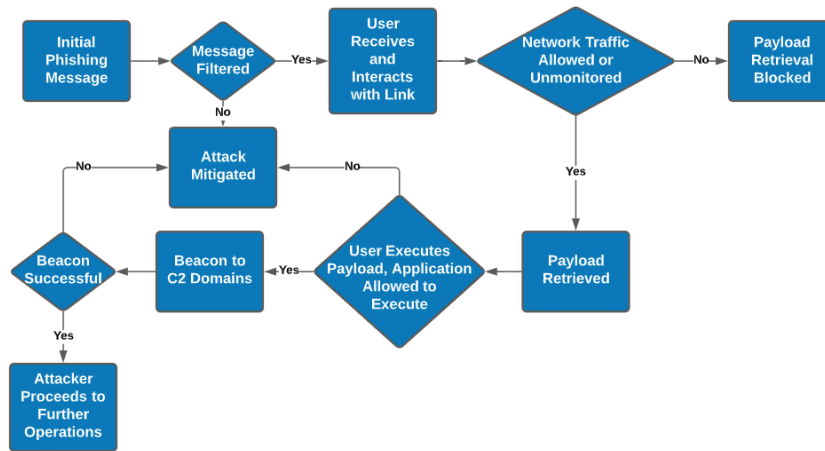
### Defensive Recommendations and Mitigations

We have already discussed several examples of possible alerting items for this campaign, ranging from signing certificate observables to infrastructure commonalities. However, network defenders must be attuned and responsive to a variety of adversary “tells” in campaigns to ensure robust and complete defense from intruder operations.

First, the simple identification of new or anomalous network traffic—whether as email links, user interactions, or programmatic communication—can do wonders for network security posture. For example, all of the domains identified in the analysis so far have scored as likely malicious through the DomainTools risk-scoring algorithm. By programmatically tying network security monitoring or log capture (such as proxy logs) to a threat intelligence source such as DomainTools, defenders can rapidly identify communication to new, likely risky sources and use this as a mechanism to launch further investigations. Done in a timely fashion, this can work to disrupt ransomware actor operations and interrupt events before they proceed toward ransomware deployment.

Second, organizations must be attuned to the malicious use of code signing for the delivery of malware. In this specific campaign, the Sectigo signing authority was abused to sign malware for delivery and execution. From a defender’s perspective, we cannot completely distrust Sectigo (as it is used by many organizations), but we can identify ways to narrow our degrees of trust to reduce attack surface. Within the context of the currently discussed campaigns, identifying the “ООО” string, corresponding to “Ltd” in Russian and related languages, may be sufficient to distinguish between trusted and unknown software depending on one’s business operations. Identifying such “tells” and their implications can allow defenders to take even trusted items, such as code signing certificates, and narrow what is truly allowed or acceptable within their environments versus what is anomalous or suspicious.

Finally, the entire infection chain outlined above relies on a user interacting with a phishing message then executing an unknown binary from a cloud storage location. These items represent critical touch points for defensive response and monitoring—and user education. Through email security monitoring, organizations can identify, categorize, and filter providers for things such as landing pages and response emails to reduce attack surface. Furthermore, organizations can limit or completely block the download of files (or at least executable files) from external cloud storage locations to further reduce risk. Lastly, execution by the user of an unknown (even if signed) binary can be limited through either training or operating system controls to eliminate the ultimate stage of this attack sequence.



Overall, visibility into network communications, the ability to refine those communications with the support of external CTI sources, and combining this with host-based or malware-centric observations will enable defenders to identify, track, and hopefully mitigate potential ransomware events such as that described above. This whole-of-killchain approach, similarly documented with respect to BazarLoader by [Red Canary in 2019](#), ensures detection at various stages of adversary operations. Through concerted effort and continued refinement, defenders will be able to identify “normal” activity within their environment and set that against abnormal traffic that may be related to malicious operations. As a result, defended organizations can gain some lead time over intruders, setting up proactive or preemptive defenses to limit exposure to campaigns as they materialize.

## Conclusion

In this analysis, we identified an initial campaign and used related items to reveal a slightly earlier ransomware campaign likely related to the same adversary. By applying this process in a continuous, iterative fashion, we as network defenders and CTI professionals can continually reduce the scope and degree of movement for adversaries and improve the prospects of network defense. Marrying network security monitoring with network indicator enrichment through sources such as DomainTools can reveal campaigns in progress, while subsequent relations to file-based observations can cement these views to enable holistic network defense. Ultimately, network defenders must leverage all sources available to them in order to adequately respond to and detect such threats, with the goal of minimizing adversary dwell time and maximizing defender opportunities for response and recovery.

No items found.

---

Source: <https://www.domaintools.com/resources/blog/tracking-a-trickbot-related-ransomware-incident>