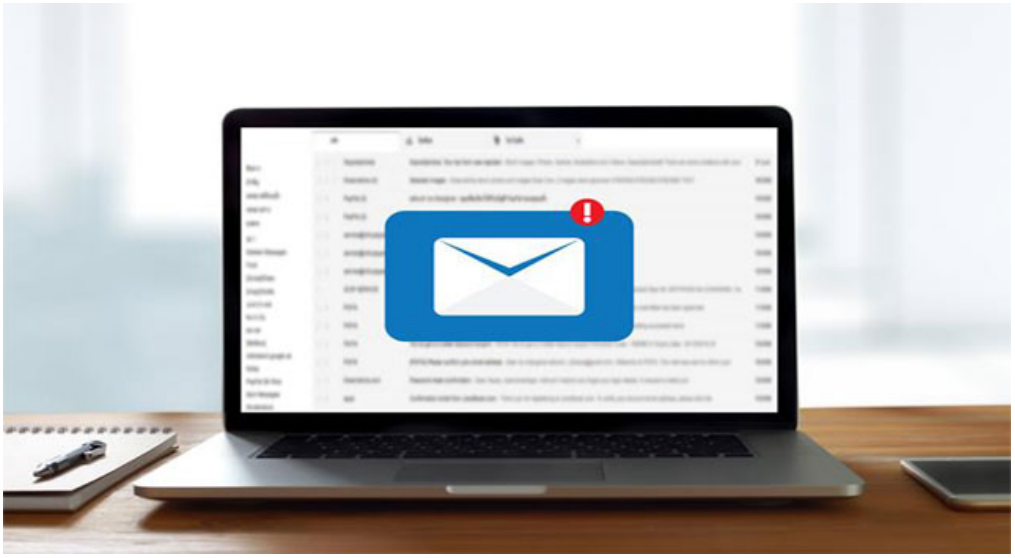
A Spike in BazarCall and IcedID Activity Detected in March

trendmicro.com/en_us/research/21/d/a-spike-in-bazarcall-and-icedid-activity.html

April 12, 2021



Spam

We discuss the cases of BazarCall and IcedID we observed in March. Both are known for the use of spam to deliver their payloads.

By: Raphael Centeno, Don Ovid Ladores, Lala Manly, Junestherry Salvador, Frankylnn Uy April 12, 2021 Read time: (words)

We observed a spike in BazarCall and IcedID activity in March. One thing these two campaigns have in common is the use of spam that lead victims into downloading malicious files. BazarCall takes a more roundabout approach by involving phone calls in its campaigns, while IcedID stole and repurposed real email conversations to make its malicious spam more convincing.

Based on separate reports on BazarCall and IcedID, both have been actively distributed through spam campaigns in March. This is also reflected in our own findings.

BazarCall

BazarCall was named for its use of phone operators to instruct users into downloading a malicious file that typically leads to the payload BazarLoader. BazarLoader was discovered in 2020 and is linked to the developers of Trickbot as well as in campaigns involving the well-known Ryuk ransomware.

We saw a surge in its activity in March, with most of its targeted victims residing in the US, followed by Germany and India, based on the number of spam mail containing BazarCall that we have detected.

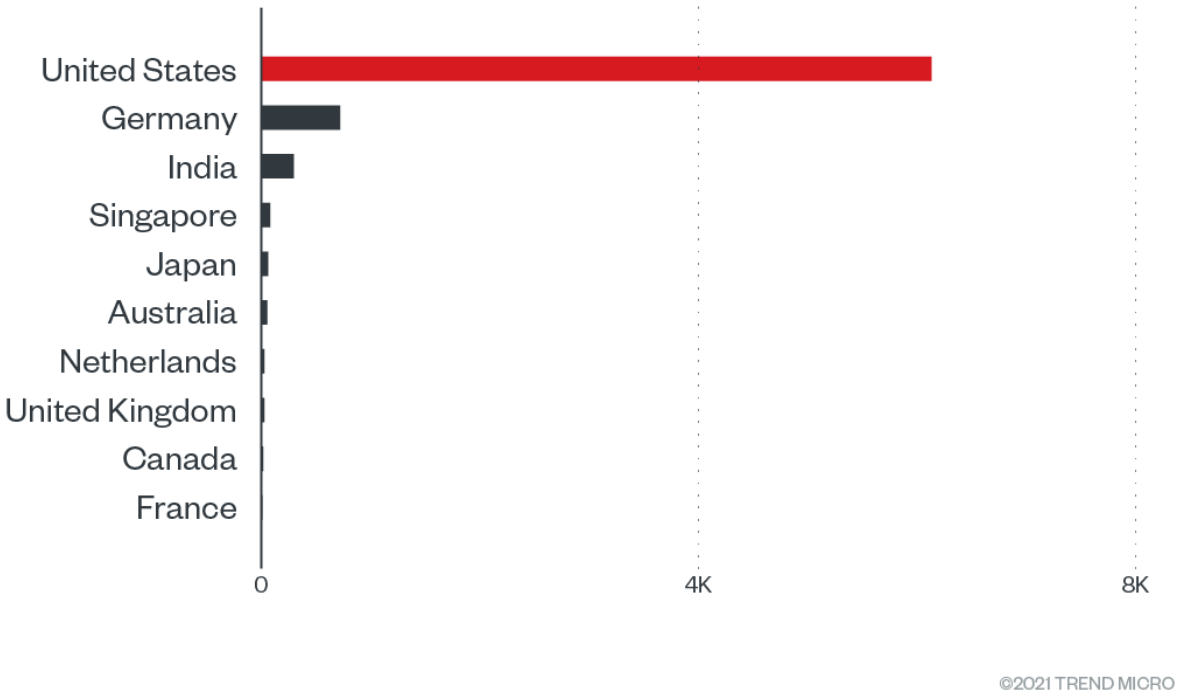


Figure 1. Countries that received the most spam mail containing BazarCall from March 23 to 25

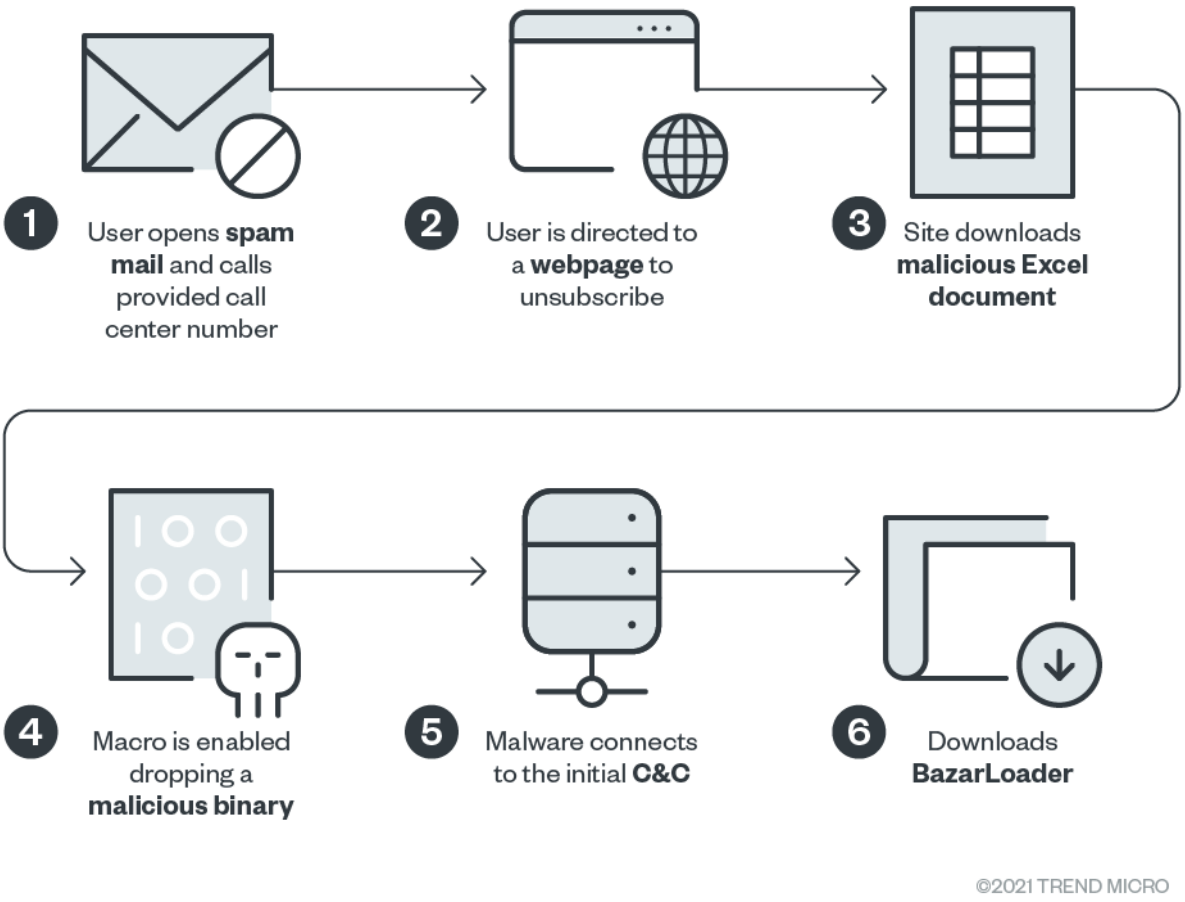


Figure 2. BazarCall infection chain

BazarCall's routine starts with a spam mail stating that the victim's free trial period for a service rendered by the fictitious company "Medical Reminder Service" is about to end. This is the same company name used in the BazarCall campaign that Bleeping Computer reported. The campaign we have observed largely follows the pattern described in their report. In the email, the user is directed to call a provided phone number to unsubscribe and avoid being billed monthly charges.

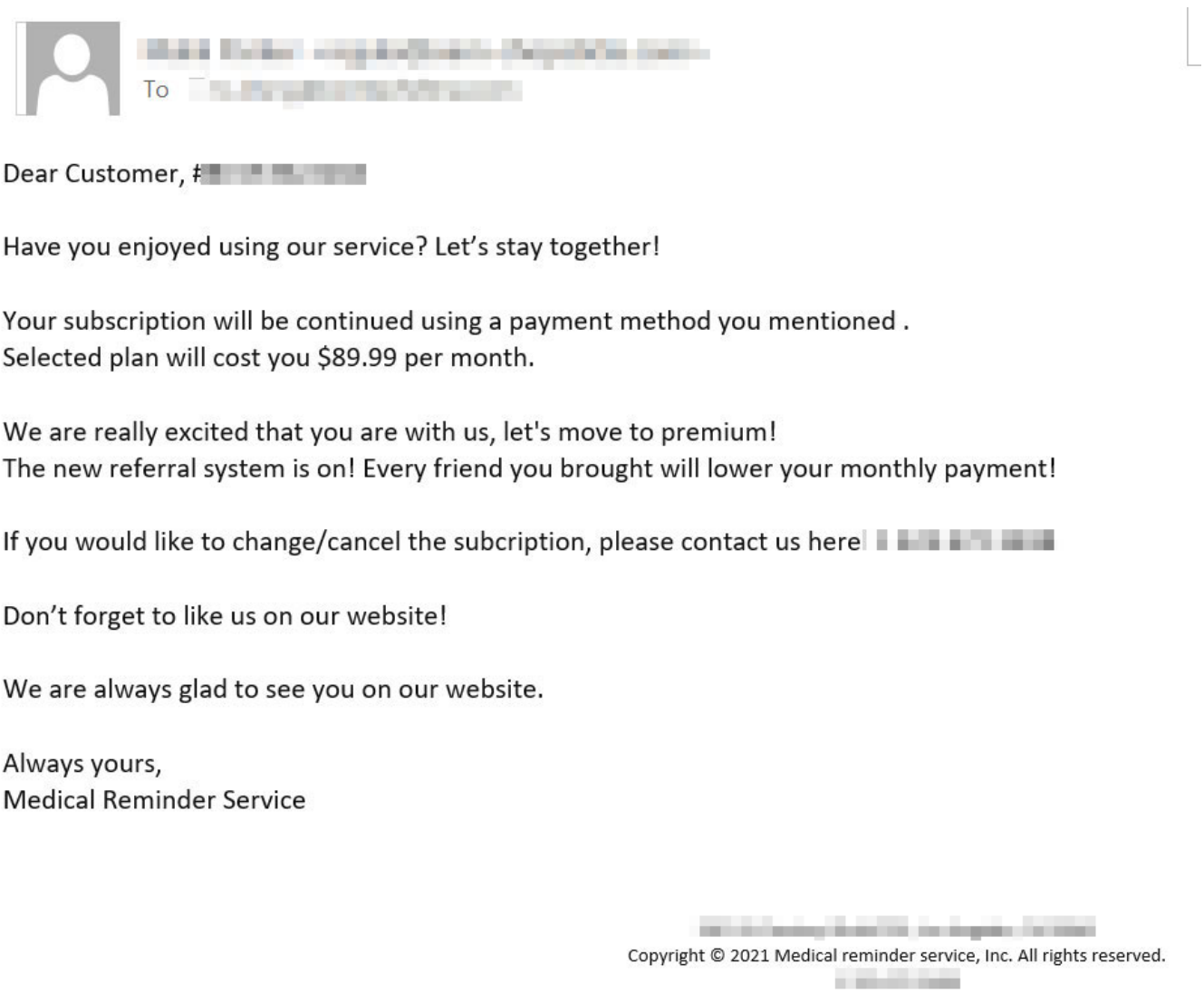


Figure 3. The message stating that the victim’s free trial subscription is about to end and the contact number to end the subscription

The phone operators will then instruct the user to go to a webpage to unsubscribe. This page is the malware chain’s download page. Once the victim enters their subscription number, the site automatically downloads an Excel document that is made to look like a regular form, but it’s actually a malware-embedded file.

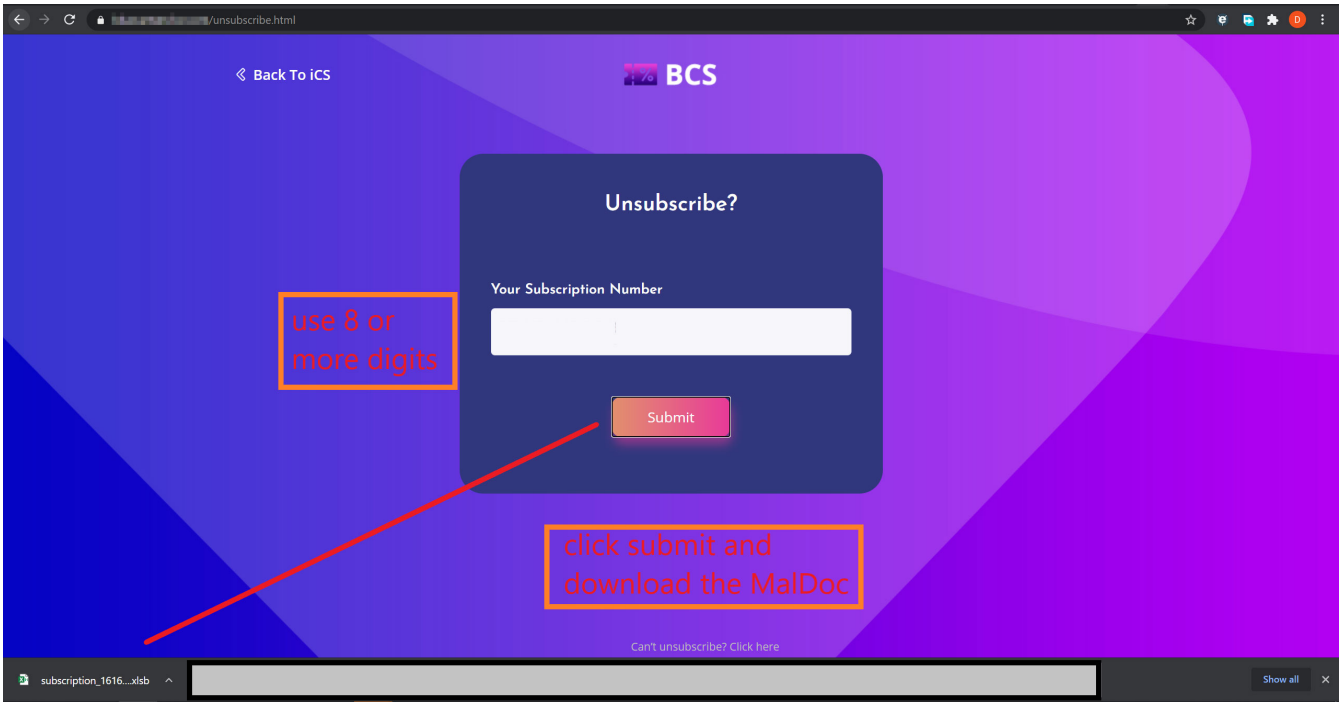


Figure 4. The subscription site and the download page for the malicious file

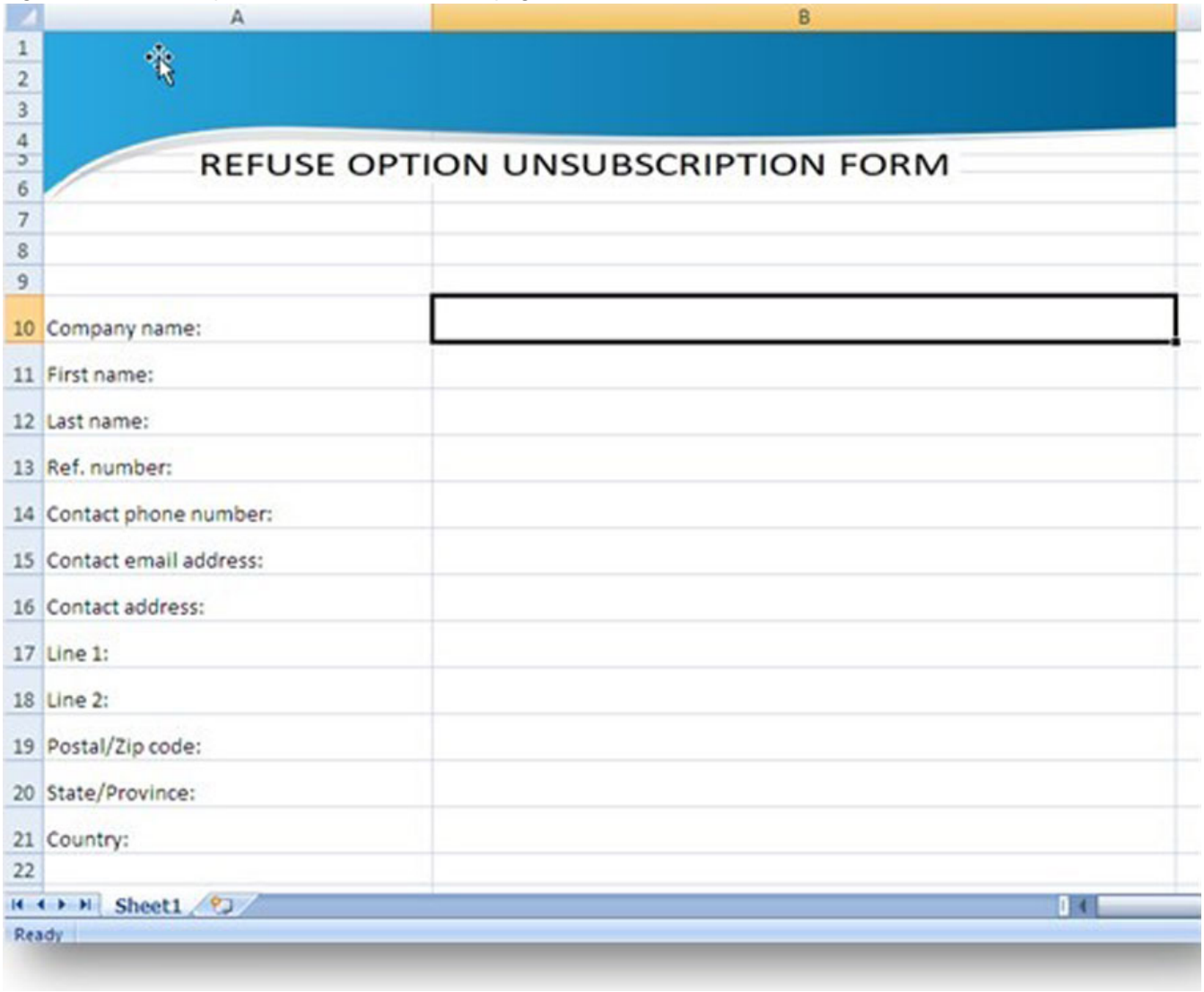


Figure 5. The malicious Excel document

The phone operator continues to guide the user into unwittingly enabling macros that will drop a malicious binary in the folder C:\Users\Public.

The embedded malware will first attempt to send the command “ping” to the initial command-and-control (C&C) server where the likely response is the second stage download URL, delivering the final BazarLoader payload. Unfortunately, at the time of our analysis, we were unable to test any of the C&C servers for live activity.

BazarCall also distinctly makes use of Campo Loader, which appears to be a malware-as-a-service (MaaS), to deliver its final BazarLoader payload. We continue to monitor developments for BazarCall. At present, the surge we saw in March seems to have tapered off in April.

IcedID

Meanwhile, IcedID is a banking trojan first discovered in 2017. It has been used by the threat group Shathak or TA551 in 2020. The group used malicious spam that contains a password-protected Word document with malicious macros.

Similar to BazarCall, we saw a spike in IcedID activity last month. IcedID campaigns are known for using stolen real email conversations on which they attach their malicious files in zip format. This was the same tactic we observed.

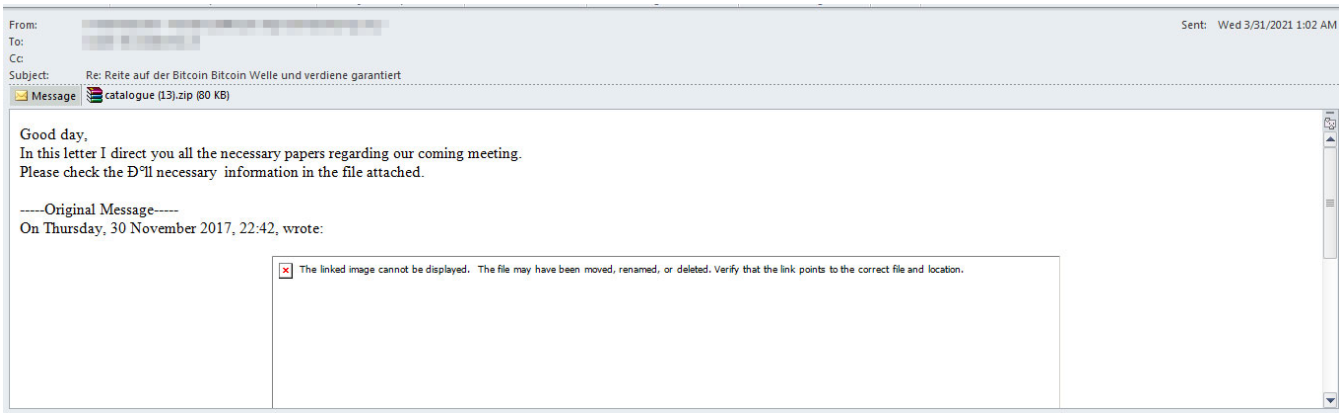


Figure 6. Sample of spam used to deliver IcedID. It is a copied message containing a compressed attachment.
If the attachment is opened it would contain an XLSM file. This file uses a simple stealth technique — a hidden column containing malicious formulas in white text, making it invisible to the victim unless they unhide and highlight the column. If the victim runs the macro code, it will download a 64-bit .dll file, which is the IcedID in binary.

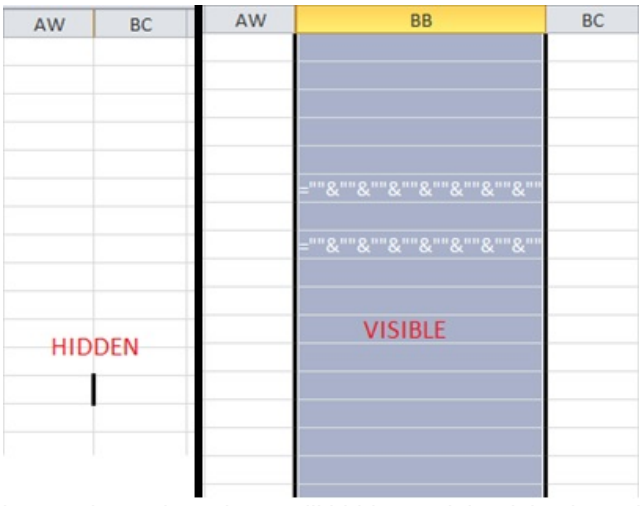


Figure 7. The Excel file used to download IcedID: The left image shows the column still hidden and the right shows it visible and highlighted.
Our detections for IcedID show continuing activity going into April but as with BazarCall, these have also decreased in number.

Implications and security recommendations

The use of spam is a traditional and staple way of delivering malware. Attacks that use such methods can resurge whenever threat actors find a way to make their fake instructions and messages more convincing. Threat actors are also on the lookout for situations where users are especially susceptible to such schemes. Remote work conditions or the use of timely topics, for example, can make users less vigilant.

These scenarios are exemplified by BazarCall and IcedID. The use of phone calls and the BazarCall operators' adoption of a regular company identity has had victims convinced of the bogus service and subscription. While IcedID's continued use of stolen conversations allows it to avoid many of the usual indicators of a malicious email. IcedID has also recently used emails centered on the Covid-19 pandemic to trick its victims.

Users need to be especially wary of the tactics that BazarLoader and IcedID employ as they have also been used to deliver other payloads such as well-known ransomware families. As mentioned earlier, BazarLoader has already been linked to Ryuk. IcedID was very recently used to deliver Sodinokibi, and was used in Egregor ransomware attacks.

Here are some of the best practices businesses and users can adopt to defend against threats such as BazarCall and IcedID:

- Always check the email sender, subject, and body for anything suspicious before downloading and opening email attachments. Be wary of unsolicited emails with unknown senders.
- Check the file extension of the attached file and make sure it is in the intended file format.
- Only activate macro for any attached Microsoft Office files when necessary. Be especially wary of emails that request macro activation using an image of the body of the opened file or those that don't show anything.
- Watch out for spoofed domains embedded in emails before opening them and do a quick search of the company or website used in emails to check their legitimacy.

Trend Micro solutions

Organizations can benefit from having Trend Micro™ endpoint solutions such as Trend Micro Smart Protection Suites and Worry-Free™ Business Security. These can protect users and businesses from threats by detecting malicious files and spammed messages as well as blocking all related malicious URLs. The Trend Micro Deep Discovery™ solution has an email inspection layer that can protect enterprises and users by detecting malicious attachments and URLs.

Trend Micro Email Security delivers continuously updated protection to stop spam, malware, spear phishing, ransomware, and advanced targeted attacks before they reach the network. It protects Microsoft Exchange, Microsoft Office 365, Google Apps, and other hosted and on-premises email solutions.

Phish Insight provides the most effective phishing simulations and cybersecurity awareness training modules on the market. Powered by Trend Micro, the Phish Insight team creates a simulation template library based on billions of real phishing samples as well as a fully automated and staggered delivery system that makes the simulation emails even more convincing. Not only integrating the best and the most prevalent training modules from around the world, Phish Insight also allows users to customize their own training programs. Phish Insight enhances information security awareness for organizations by empowering people to recognize and protect themselves against the latest cyber threats.

Indicators of Compromise (IOCs)

BazarCall

SHA256	Detection
056809e596895320397378f7f3ff4958107e48f4890a960229dcfbc32b7379b7	Trojan.X97M.BAZAR.YABCZ
0606be9a1e3e32dc452cdd0ee48c3cecdb045545fa01789f580c197cefd220a4	Trojan.X97M.BAZAR.YABCY

06c38b4c73015d04536d80262bb531183bead459371dd6db86a40dfccbdf236a	Trojan.X97M.BAZAR.YABCY
0e266ef60c8059c2c828de3e77fd68a49e50626d7b0d4d659afd03806247d5bc	Trojan.X97M.BAZAR.YABCYT
13141db5db00c63f5f7a2cd33f35d9236956f9ae7767725564693dbab6b14f10	Trojan.X100M.BAZAR.YEBCX
151308d22127e12066636627acb269e6ac71aa99cca1ac9dd00b582de3b5e0cd	Trojan.X97M.BAZAR.YABCY
15a1cd485f5b09fa05c46ec81d7eaaaa1e71bfd3b19e3465f555704dbfadce31	Trojan.X102M.BAZAR.YEBCX
1681ae715209131c86f885453e3abd627de1edab974294b73789dfd396d2793e	Trojan.X97M.BAZAR.YEBCW
16bfc0c0fcb0ccb6bb27cdc4178d08538c0b18c146d93a3a44be5fb15d8d43cb	Trojan.X97M.BAZAR.YABCY
1c293c65680d01a8503c477f7d8f46cfbc62ce4fa6e507a4c0ae7436f33efa08	Trojan.X97M.BAZAR.YEBCX
1eba154cdc2e540704eebfaca2f51fb643c44129911eb9b668f82ab95c1b157d	Trojan.Win64.BAZARLOADER.YABCY
2032cca770ec5bb02896b5b098f00564add5a5ee528973aa264fa85cdb1b1375	TrojanSpy.Win32.EMOTET.YABCY
204ddd2c357d7d5a5d30761f2da8363a3d26e1717e90ccc69b00b7be456f4092	Trojan.X97M.BAZAR.YEBCX
20cd67833a009771483fed52ad8450d1614df7843715eb67250dd605780d1e8b	Trojan.X97M.BAZAR.YABCY
227b402fe1ad5c40edd6385590dd22add3e493be6c90c813786a1d2a92c5508b	Trojan.X97M.BAZAR.YABCYT
27cbaa0a743ded5ed298ba18bb2bca3c9cf605a9d75f7168ea7cc00ac54687b2	Trojan.X98M.BAZAR.YEBCX
2ae9a949242e7691ea1df0475a0f266118dc382fd27350b575473d9da9d9fc1f	Trojan.X97M.BAZAR.YABCYT
2c9787310c6307f1d169c5dff44455a52a5da01681b45f6ad9c382334c431400	Trojan.X97M.BAZAR.YABCZ
2fcc02b25bfccda87b03b1149eeb22379abb5b00f2ea474151979f87ee6a8289	Trojan.X97M.BAZAR.YABCYT
3369c4b31d3b5904783ee651d94d78995aa8ac2d6d4b52bc455c17c75845efbd	Trojan.X97M.BAZAR.YABCYT
3866ad9640aefdefb66843ed3151d95007d76a7254e41d9a17389656a97afc80	TrojanSpy.Win32.EMOTET.YABCY
391c2301f9c1b27b489b78bac987e2e61e7923da1342941f3f52618e2d1ee1f8	Trojan.X97M.BAZAR.YABCYT
39e79fa4dffb5d3c4099ccd77f9a889a7a0179948862790aeba79c69ffeb8582	Trojan.X97M.BAZAR.YABCY
3a274a44ca7e8c943f9a2d1995d97582886d8f9684b7d5c5b51625f9f833d7ec	Trojan.X97M.BAZAR.YABCYT
3eda5bc62ee17d2ba137c4253eacfd9f96926ec071eb583777935c084cdcb604	Trojan.X97M.BAZAR.YABCYT

403e6317c3ef24bdacd6ff265a5b93cf43361398cba8918af459fb7072fd8ceb	Trojan.X97M.BAZAR.YABCYT
413ca9be6e90c35d5e680ea00891976673cd22446ca31c3dc4e678356737d75c	Trojan.X97M.BAZAR.YABCYT
43af28b1e4057888f074b01ddce13b6445b530cf70741d3e3bb65a712dc58775	Trojan.X97M.BAZAR.YEBCX
4435942b9f09846a337474f396fd0a885f41742f05899dcc1a12b6b44a31126b	Trojan.X97M.BAZAR.YABCYT
461172b3e91e48945f91e7cb507f02d391bee5b2736ab33ef87c4068da99cabf	Trojan.X97M.BAZAR.YABCY
4d1c7b33d3dd2ec8187bf29971a3785a9103a4dbd97cad37d6fd16f4dc761c0a	Trojan.X97M.BAZAR.YABCY
4e58b94d857970b01c70e8fb4c68c99a409c5eb105e286f521325eb209e19a59	Trojan.X97M.BAZAR.YABCY
580436ddf51ed876d2e1547047288b0640bfd7570ffd7a2ef9074b116ad5f823	Trojan.X97M.BAZAR.YABCY
5b6e4db97888c248d70e6a2ecfe4967b5bb3ffba3e73fc04fcc91da8afe37f81	Trojan.X97M.BAZAR.YABCYT
5c03e5522fb03bc224b51be1206728e4cfc5ab6b5a45555c455819e8b5006356	Trojan.X97M.BAZAR.YABCYT
5c7a7b0b29a2f51eca70e25936b2f88570b44b0aef504d07b208621df0022103	Trojan.X97M.BAZAR.YABCY
5ee9bc24c82ee40e1a9f98aff8e36388ccea92a9423539e13b927291bebede72	Trojan.X97M.BAZAR.YABCYT
624a74c9469e95f404baebd07a8c563baa38e752d391bca5e8894dbc87186388	Trojan.Win64.BAZARLOADER.YABCX
6529aee58be4346065cf8f5166c49ecd7dbecfeb179092d0ba9ee4fecbbb0f8d	Trojan.X97M.BAZAR.YABCYT
67b5ef18a2155a91980d6ecd5ce2fb73242b47921715095565ba5e7d97922aa6	Trojan.X97M.BAZAR.YABCY
683cf783dffa8ce135496f8f5017fc06268c57874ad79267cb52dfc202dfc3bc	Trojan.X97M.BAZAR.YABCYT
701ff2df2c26f4ec31eb39074e0f7da97ad9f8e7e0877558571148db64a343cf	Trojan.X97M.BAZAR.YABCY
739a35cdd227b78b2a3f49dff22b9185df7b6da1336dccd0c6f552ae0767397c	Trojan.X97M.BAZAR.YEBCX
825e158ac8c57cee3a2d12ba062633e7a955e20d438b6b1b89c435181586a0ef	Trojan.X97M.BAZAR.YABCYT
8300b9b7de6fd356541b30ed343c00235bf38fbcbe2325ecd4b6f06b2b711f03	Trojan.X97M.BAZAR.YABCY
8a6adc186c65c1db9026fa07e02e813e059a1463fc89b05c4440e2ddb143bd46	Trojan.X97M.BAZAR.YABCYT
8a9014b5a7e0975e760ebb41b5d6cac6e76bf1b3b5c2cb0dfebd94e577a6940b	Trojan.X97M.BAZAR.YABCYT
8c908237c4354e3f96af0944dc84fd1d503827226f914a5e711f5415b1cec156	Trojan.X97M.BAZAR.YABCY

8ca38418522c7797e0e2fcf8649b3adb64b70f9ad547f7cdc53a55cacacc0b4e	Trojan.X97M.BAZAR.YABCYT
931a10977e46a3a1c810c1e3dad558b511a8fc75bd30e2eb3ffe292428f99847	Trojan.X97M.BAZAR.YABCYT
94ab1b1ca2123fccd39b956c9216f53ba56c012553281801d4af035dc1644569	Trojan.X97M.BAZAR.YABCY
95330c3095995c4e018936438d2f6da39cd55d29c52438c8042d39118ac81dc9	Trojan.X97M.BAZAR.YABCZ
95c9b5f666e90730d21e342aeac6f101d9c624ace3bd4e8bd7d5d9c541094283	Trojan.X97M.BAZAR.YABCY
98a54d72539d50134f8e95fb95d3807502ca50c2f27990a220c78432a799d461	Trojan.X97M.BAZAR.YABCY
9aa42472f59e5558987ce477e257fdccd61080d4278fe9a92f1c50bda11e4f0f	Trojan.X97M.BAZAR.YABCY
9cc79e32ca74fea9e6a9ed7ab09abfa33d0fb2c3ef8752baed056de05f4b2de6	Trojan.X97M.BAZAR.YABCYT
9d6581dbec6c8f74f2d999b5b72a8d8f515bd71c1d0966754374b8a16d3c4bd7	Trojan.X97M.BAZAR.YEBCW
a05ec823e486a21a5cea8811115ae750c9796f918228566463ed9a9f712238c7	Trojan.X97M.BAZAR.YABCY
a144bdfb007c72eaab61f424725107366747afc2252675e2a8992401f581f2b5	Trojan.X97M.BAZAR.YABCYT
a14e4ee9f2967d2189e7b725cbb7156a5132f55e96ce6497ac0a582d3a696510	Trojan.X97M.BAZAR.YABCYT
a839e6e8570d4e836ef03ced53d77217cbd3f08558582733da8f60b0a0e6fa83	Trojan.X97M.BAZAR.YEBCX
adbb324ef7beb35f9ea52e92b3cc613f8082ba9d	Trojan.X97M.BAZAR.YABCZ
b17773d67198e8ca31b2029789fdbf034dbe7d65e3425dae9c02638fd1da33ee	Trojan.X97M.BAZAR.YABCYT
b4631d97013e59555487c6c4c93798dd044e8268858eb031f6c324039cdff962	Trojan.X97M.BAZAR.YABCY
b4b5161dbce88e4f35a58921fa4e81b9231e2ab92d6e80091bfd9ef4574ef822	Trojan.X103M.BAZAR.YEBCX
b4d956e037fd49630847b92997906c14d76513ae2f00ffe8ba40d9fd5dae98ad	Trojan.X97M.BAZAR.YEBCX
bb9387320d69ddd3e4cd4586ae85ffd672d241d112e0199eeda0e59634aea4b0	Trojan.X97M.BAZAR.YABCYT
bc604d1564b8b0360eb316b6d330d069dd887875db3d1c0cc1e6e8b6d044fa84	Trojan.X97M.BAZAR.YABCY
bcfd5b1ab6019b320a299ec62374df157162116b7ab76d2dd852075b2df36d06	Trojan.X97M.BAZAR.YABCY
be0466432cbd09f14c01975d9cbf24ce3539fd245918bd1b567d3cdda8f76324	Trojan.X97M.BAZAR.YABCYT
c1d2ac7f3abee76af28e858f9d9b5c26bd121bc298280f44cb06e00951cb28d7	Trojan.X97M.BAZAR.YABCYT

c242a240f6836d70944d4810c9fbc4b2ee7221c5938f483d1ab8579955a4c78f	Trojan.X97M.BAZAR.YEBCX
c8768444c9e489989a6610537ecb1bc204216e0b0880079e6d9e561e56dc60a8	Trojan.Win64.BAZALOADER.YABCW
c8d4265b3762f38162e9b93563bccf603081de769b9c5c38d41b65872d0c944c	Trojan.X97M.BAZAR.YABCYT
cd0332bed798951f6e1635b6169e07c41138323490e52fa9f674b6a113156a34	Trojan.X97M.BAZAR.YABCZ
ce8fa7b1fbc88467678f3d2877c5580a5bf310cc489536a3aaef3f9b8d1db992	Trojan.X97M.BAZAR.YEBCX
d021f3c83a2fb22da832e301962d63c695194907ab415d0b978858699e22952a	Trojan.X97M.BAZAR.YEBCW
d4723b2d858287cb8c01f64a00970f089be96ad886e83a1da38e84325fc9b886	Trojan.X97M.BAZAR.YABCY
d49953673284c656971ba15caf8a1cc07902ae972836bd282a20aca916d15e45	Trojan.X97M.BAZAR.YABCY
d8bcb2ec7da1dd5ea941807b790aa7dfdab9291e1cdc80fee3dc1d6e3b6981e2	Trojan.X99M.BAZAR.YEBCX
d92bf3350a4b310ab6b7d295a0d1727155ec6d669b2da021c91aa9b565593a7b	Trojan.X101M.BAZAR.YEBCX
d969d06464b2c8eab75bf45e650020cc88add0bc947643dd24d69bbf34481906	Trojan.X97M.BAZAR.YABCY
df38d84cefcaf27b357bf0c678ab22531d5e2886658f5482e9ace04a315828e6	Trojan.X97M.BAZAR.YABCYT
e335e27175c66affc5c2b571878757b35642699b70250c4221800e47356d4b59	Trojan.X97M.BAZAR.YEBCX
e4782e0fcb58e3643a293e9792be9d33b2147c96824c110105a198602c587d47	Trojan.X97M.BAZAR.YABCY
e8c6014607b1160a2efa1ebc35f71e73e7e08c1e027d8128d985729b61c3d203	Trojan.X97M.BAZAR.YABCY
e99a54ca11fd5e27c5085c24304103a348fa2a550ea1fa934fca541551c511d6	Trojan.Win64.BAZARLOADER.YABCX
ecf5a6e4dfd2bc3a9a659699ee03e6c5ebcbd3252664245761f1594044f0c5fa	Trojan.X97M.BAZAR.YABCW
ee9ba17fb42f85ed79f5a9f15673327579538de8eb268ea134b97bff3f54c44c	Trojan.X97M.BAZAR.YABCZ
f2853ce6b6515446daf068272aba80c2c059f2c20e197f32060b9baf6bbd17a2	Trojan.X97M.BAZAR.YABCYT
f3badf0a258410c281afe6ac253cbd48b1b4be6a656db60813131a3025cd8d11	Trojan.X97M.BAZAR.YABCZ
f6391f0bb648e3821d88179b2f76426197961c739b7ad88329a91d5a1328cc61	Trojan.X97M.BAZAR.YABCYT
f8662af41f8a99a17220a0181c3d4c5fd82ca6b522c5da4856f03accf3838a72	Trojan.X97M.BAZAR.YABCY
fc3d3e2e605e76289cecb3612bd000471e613bf8841cc4e9c6b9f47b527a3d6a	Trojan.X97M.BAZAR.YABCZ

fd93b2dd5067d6933d9d06878c75b53bdba8756f092c4ccb1e9ce881bb1ec85c	Trojan.X97M.BAZAR.YABCY
fee876283fdd75a8ea08d19c15e9c78755a8cc3135d157609097d2b249e0e7fc	Trojan.X97M.BAZAR.YABCY

C&C servers:

- hxxp://18[.]220[.]10[.]246
- hxxp://52[.]90[.]97[.]160
- hxxps://35[.]168[.]81[.]240
- hxxps://52[.]167[.]249[.]196
- hxxps://52[.]90[.]97[.]160

IcedID

SHA256	Detection name
219e7715d364c0a46c667bdb93b05776f257da38028cbaa5a504873eb166315a	Trojan.XF.ICEDID.THCCABA
89756db6627e4c3ab511a0a6efe68dcfb6bec881c4942331dc95d53435e8f38b	Trojan.Win64.ICEDID.THCCABA
8de416bd5b7913a0f58610c56f0fdb293873a069522024f281c2e0106fd74042	Trojan.XF.ICEDID.THCCABA
a1411ad0725807a327258b5520ac7c1b709878ca84a6d2ee1d7a9913833b7429	Trojan.Win64.ICEDID.THCCABA
a1411ad0725807a327258b5520ac7c1b709878ca84a6d2ee1d7a9913833b7429	Trojan.Win64.ICEDID.THCCABA
a2fcccd77c387840adb0de73b7361fa8a230c4a50ef309c1353fb499004272fb	Trojan.XF.ICEDID.THCCABA
cb5864f279f49a06becdbcc287925d6073a4b72798daba165433a75d2bb3b0f9	Trojan.Win64.ICEDID.THCCABA
2f0dc07dc3a2ca82ee1ba3c92c83c1702d1dea8fe363d4f224b399377ab50e51	Trojan.Win64.ICEDID.THCCABA
442b31da9f6c4ffedd0a0d40a725c966a3c25284a0903ef40e2d0aa6bd8bfdaa	Trojan.Win64.ICEDID.THCCABA
47eafc7cbd120f040b93ce9e682de907f3a9fe8a78ec187f5af48039fd55ce5f	Trojan.XF.ICEDID.THCCABA
54efde21d125c3f0d057e89c4c10960d925b14253b59cfbbcda03a7e9d80fabc	Trojan.XF.ICEDID.THCCABA
56b6eaacab819f6199b96b06510eebeb30f99adcd559e3c87111a18d1ca6ed76	Trojan.Win64.ICEDID.THCCABA
6d7751eb2aea2a561e5e33a951cc43d70b1f0c20054b60b8f1004aa36dc4dccc	Trojan.XF.ICEDID.THCCABA
89756db6627e4c3ab511a0a6efe68dcfb6bec881c4942331dc95d53435e8f38b	Trojan.Win64.ICEDID.THCCABA
9052448c8250fdf0b739d16b30d8d6807b1223a7e919d4f1f09a4ba5f847e74a	Trojan.Win64.ICEDID.THCCABA
9cbf18d067a292361999b12af131ebf575d1d8acf21a58e55b2837a3621aeb2f	Trojan.Win64.ICEDID.THCCABA

a2e4dc07cc85543b86e7c46887e7f96626e2cd9993e0787daa7b963a7e1b324c	Trojan.Win64.ICEDID.THCCABA
ba54ae65803b5c842dbb86a7ac72167906d3d22332c7aa56f2b6b4a337a9aabb	Trojan.Win64.ICEDID.THCCABA
c0768ee6bd8a1d5a5435e2839eb54f8b6d1a120a323c51c679070a22e550b1d5	Trojan.XF.ICEDID.THCCABA
d258d95c4ca5e71cf03f7952bb53876a730c12f3def5918beb3862aacc39f0d6	Trojan.XF.ICEDID.THCCABA
d86405130184186154daa4a5132dd1364ab05d1f14034c7f0a0cda690a91116d	Trojan.XF.ICEDID.THCCABA
df4fb2147efad93deb6fbc74545bb346ff2e719f7b77830988ca15df28857a21	Trojan.Win64.ICEDID.THCCABA
e0f75a7b2d229eca6028061fe23483acd46c565b6d0e6dfa38148ad079f94aa7	Trojan.Win64.ICEDID.THCCABA
e8ad149f6e754162432b1040443269ed078d2ab027f3e93ae4b4ff8801ac8760	Trojan.Win64.ICEDID.THCCABA
eb9981fb381d6b252c1fce45b95baec5b563897b82ccc855f482f73e64e6ed46	Trojan.Win64.ICEDID.THCCABA
f8b7283ffc3cbc94cdfa193d833497c7f32611f97963a15f1ee9e4d07cc87b67	Trojan.Win64.ICEDID.THCCABA
fb7b725d0d1b47564070e0f10e237baf1f27d6f86afa11f163ae9692c85f2638	Trojan.Win64.ICEDID.THCCABA

URLs:

- hxxps://agenbolatermurah[.]com/ds/3003[.]gif
- hxxps://agenbolatermurah[.]com/ds/3003[.]gif
- hxxps://columbia[.]aula-web[.]net/ds/3003[.]gif
- hxxps://metaflip[.]io/ds/3003[.]gif
- hxxps://partsapp[.]com[.]br/ds/3003[.]gif
- hxxps://tajushariya[.]com/ds/3003[.]gif