Threat actors attempt to capitalize on coronavirus outbreak

blog.talosintelligence.com/2020/02/coronavirus-themed-malware.html

- Coronavirus is dominating the news and threat actors are taking advantage.
- Cisco Talos has found multiple malware families being distributed with Coronavirus lures and themes. This includes emotet and several RAT variants.

Executive Summary

Using the news to try and increase clicks and drive traffic is nothing new for malicious actors. We commonly see actors leveraging current news stories or events to try and increase the likelihood of infection. The biggest news currently is focused on the new virus affecting the world, with a focus on China: the coronavirus. There are countless news articles and email-based marketing campaigns going at full throttle right now, as such, we wanted to take a deeper look at how this is manifesting itself on the threat landscape.

Our investigation had several phases, first looking at the email based campaigns then pivoting into open-source intelligence sources for additional samples. These investigations uncovered a series of campaigns from the adversaries behind Emotet, along with a series of other commodity malware families using these same topics as lures, and a couple of odd documents and applications along the way. What was also striking was the amount of legitimate emails containing things like Microsoft Word documents and Excel spreadsheets related to the coronavirus. This really underscores why using these as lures is so attractive to adversaries and why organizations and individuals need to be vigilant when opening mail attachments, regardless of its origins.

What's new? Malware authors and distributors will go through any means necessary to achieve success and generate revenue and this is just the latest example. These lures tied to coronavirus are likely to only increase in volume and variety as the virus continues to spread and dominate the headlines.

How did it work? The majority of these campaigns were driven through email and malspam specifically. These actors would send coronavirus themed emails to potential victims and, in some cases, use filenames related to coronavirus as well, enticing victims to click attachments. One of the reasons this was so effective was the large amount of legitimate email related to coronavirus that also included attachments.

So What?

- Organizations need to realize that attackers are going to use current events to try and get victims to open attachments or click links. You should be prepared and vigilant in identifying these emails and ensuring they don't make it to your users inboxes.
- There is a wide variety of threats represented here so there isn't one single threat to be concerned with, just realize there will likely be a lot more.
- It's not just malicious content, there are a lot of weird executables and other files floating around that are coronavirus-themed and are unwanted, albeit not inherently malicious.

Malspam campaigns

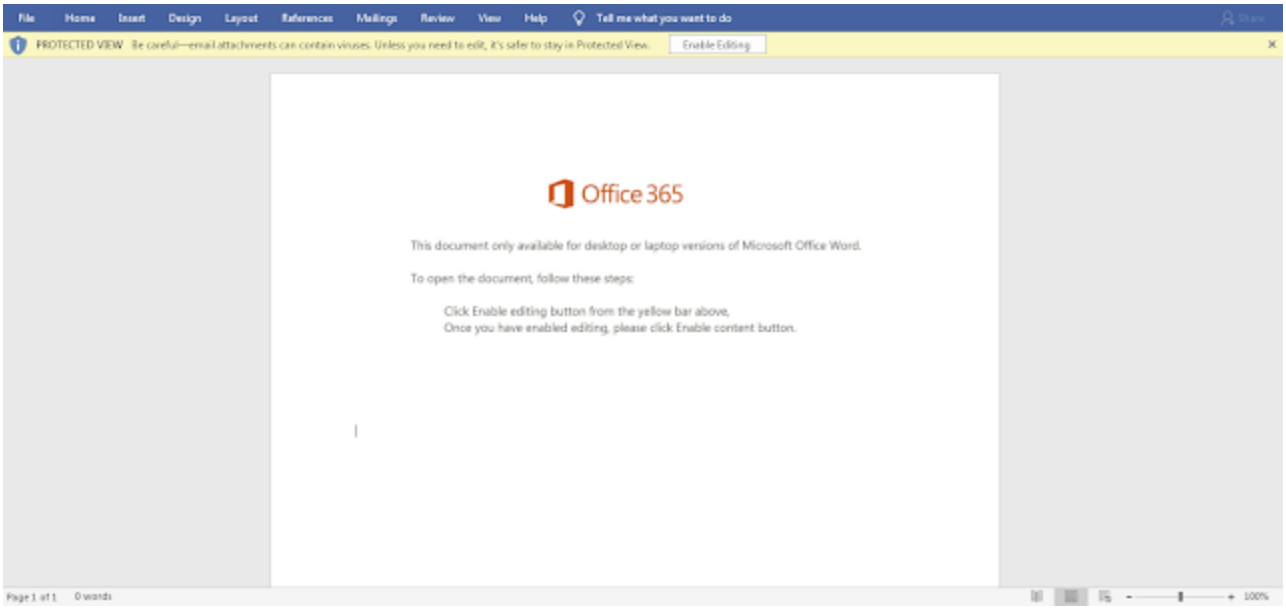
During our analysis of email telemetry, we identified several malicious spam campaigns leveraging news related to coronavirus to entice potential victims to open attachments and initiate various malware infections. Several malware families are currently being distributed via these malspam campaigns including Emotet, Nanocore RAT, and various trojans.

Emotet

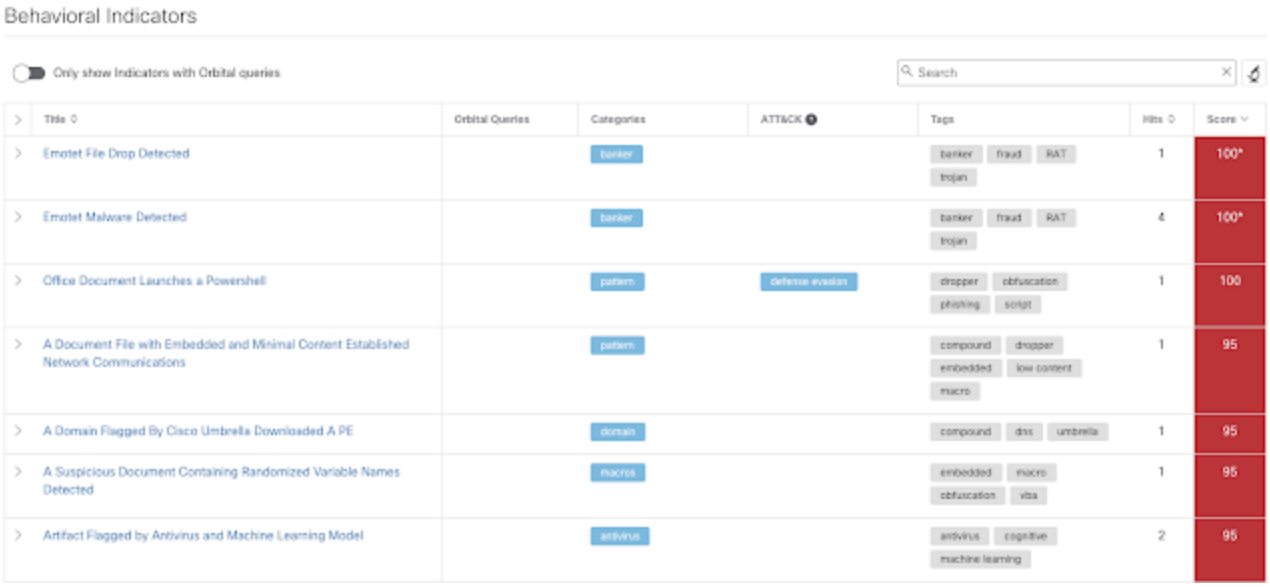
Emotet is one of the most prevalent malware families being actively distributed. We have previously analyzed this threat in various posts, notably here and here. Emotet distribution campaigns are commonly observed attempting to integrate current news topics of interest in their distribution campaigns and the current interest in CoronaVirus is no different. It has been previously reported that Emotet has been making use of this theme in various email distribution campaigns, which we have also observed. As previously described, these emails typically contain malicious Microsoft Word documents that function as downloaders for the Emotet malware.

An example of one of the malicious Word documents is below. As usual with these sort of attachments, users are prompted to Enable Editing and Enable Content, granting the

attacker the ability to execute code on the endpoint to facilitate the delivery and execution of Emotet, thus infecting the system.



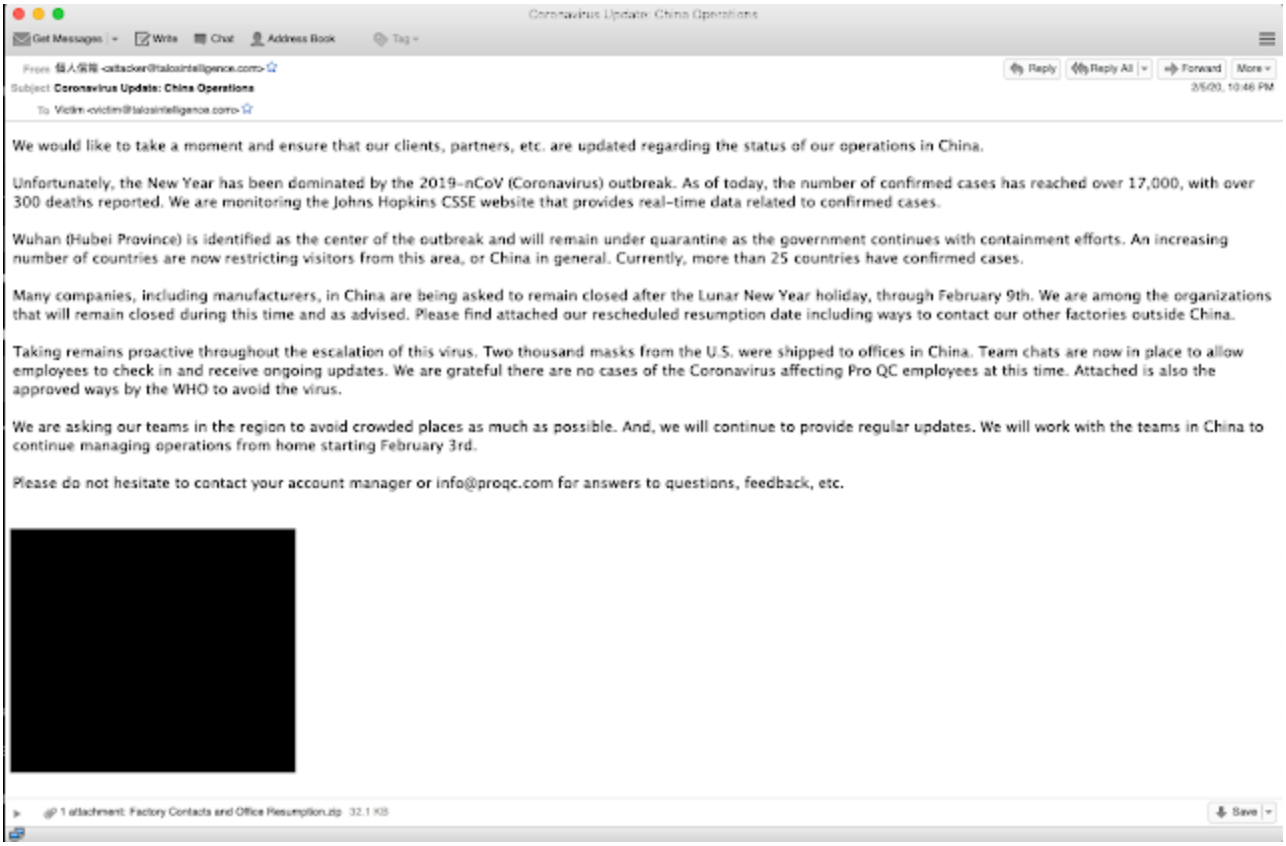
Over the course of the past few weeks, we have observed large quantities of messages featuring this and similar themes being used to spread Emotet to victims.



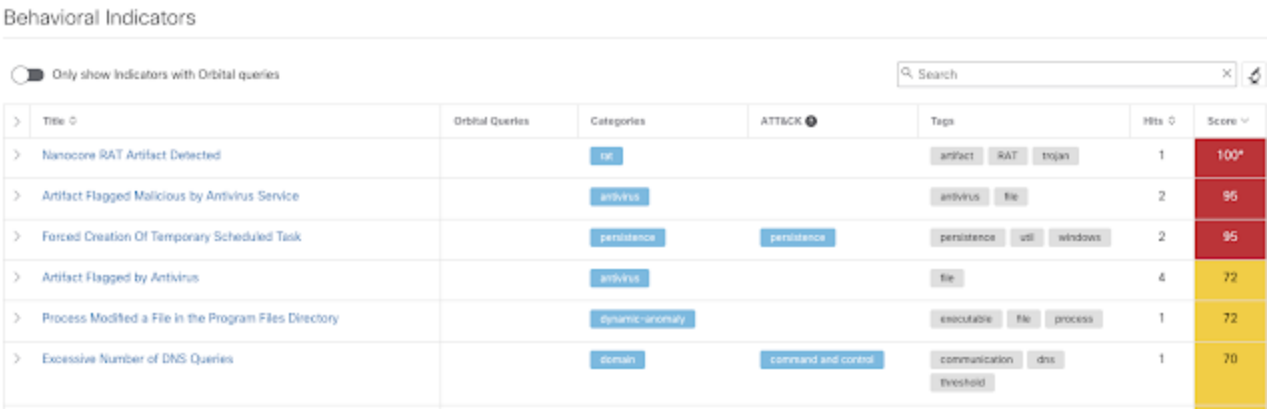
Nanocore RAT

It is important to note that Emotet is not the only malware family currently being distributed using coronavirus-themed malspam campaigns. We have also observed Nanocore RAT being distributed using similar types of email-based malware distribution campaigns. Nanocore RAT is a remote access trojan (RAT) that is commonly distributed by various threat actors. RATs are one of the more common threats we see delivered on the threat landscape. These malware families typically provide the attacker with remote access into the system and the ability to grab things like keystrokes, files, webcam feeds, and download and execute files. During our investigation we did find a campaign delivering Nanocore, one of

these RATs. The campaign was a notification to customers around the status of the coronavirus and the steps they are taking as an organization, as is shown below.

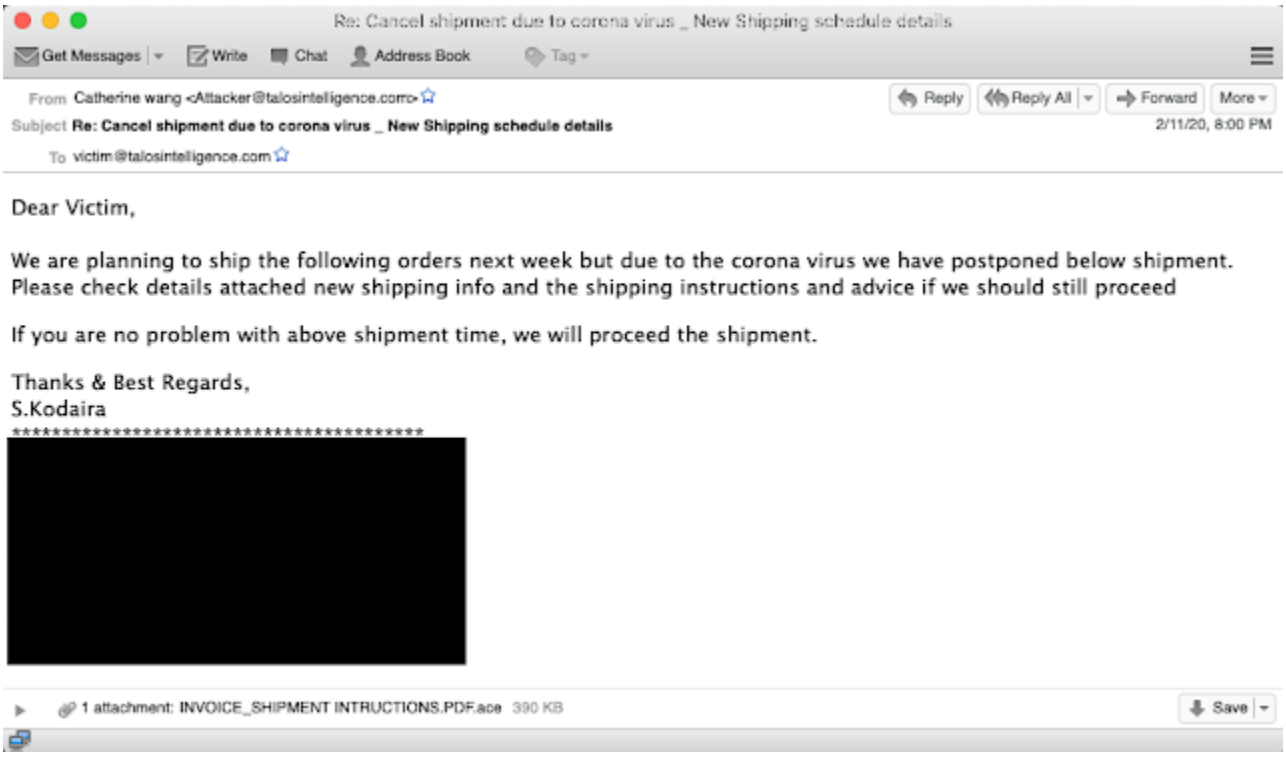


As you can see, the email came with a ZIP file attached, which contained a PIF executable. Once the victim executed the file, Nanocore RAT was installed on the system, giving the adversaries remote access.



Other campaigns

We did find at least one other campaign that was ongoing, but at the time of discovery the command and control (C2) servers were down and final payload retrieval wasn't possible, but the malicious intent was clear. This started like many of the other campaigns with a coronavirus theme.



This particular email was notifying customers of a delay in shipping due to coronavirus and attached a .pdf.ace invoice file. Inside the compressed archive was an executable purporting to be a signed order confirmation. Upon execution, additional data was attempted to be retrieved but due to the server being down, it is not possible to identify the final payload as of the time of publishing.

Additional malware campaigns

In addition to email campaigns leveraging coronavirus, we also analyzed various open-source malware repositories in an attempt to identify additional malware making use of the disease. We discovered several examples of malware that had been submitted to the repositories including adware, wipers, and other various trojans.

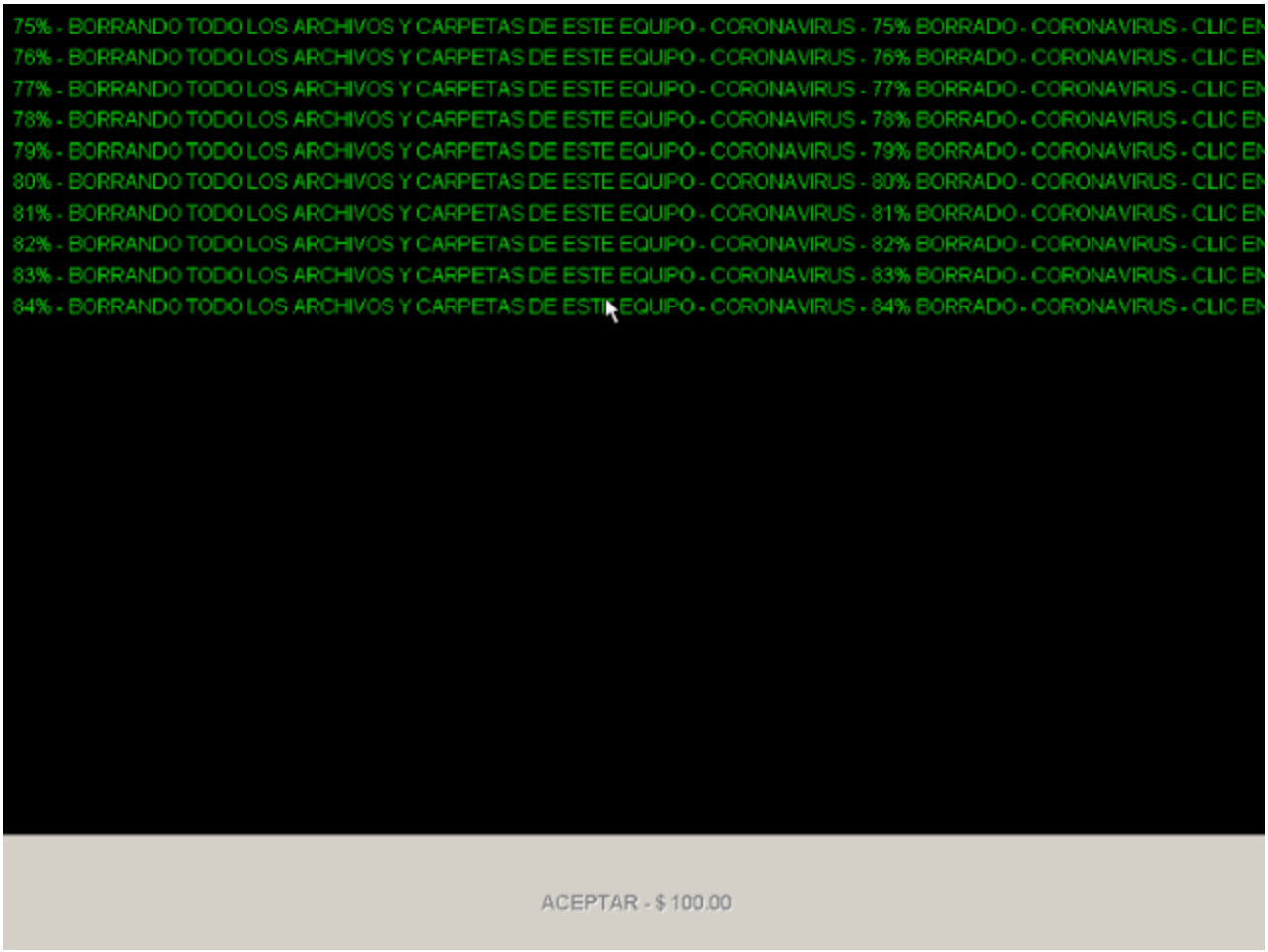
Parallax RAT

During our open-source investigation, we came across a sample aptly named "new infected CORONAVIRUS sky 03.02.2020.pif." This file was likely delivered as an attachment to an email in some sort of compressed archive. Upon execution, the RAT is installed and persistence is achieved by creating links in the user's startup folder, as well as the creation of several scheduled tasks, and establishing command and control communications with a dynamic DNS provider domain, which is fairly common with RAT distribution.

Parallax is another RAT not much different from the nanocore campaign we found above. It has the same basic functionality and allows the attacker the ability to upload and download files as well as grab things like keystrokes and screen captures.

Other samples found

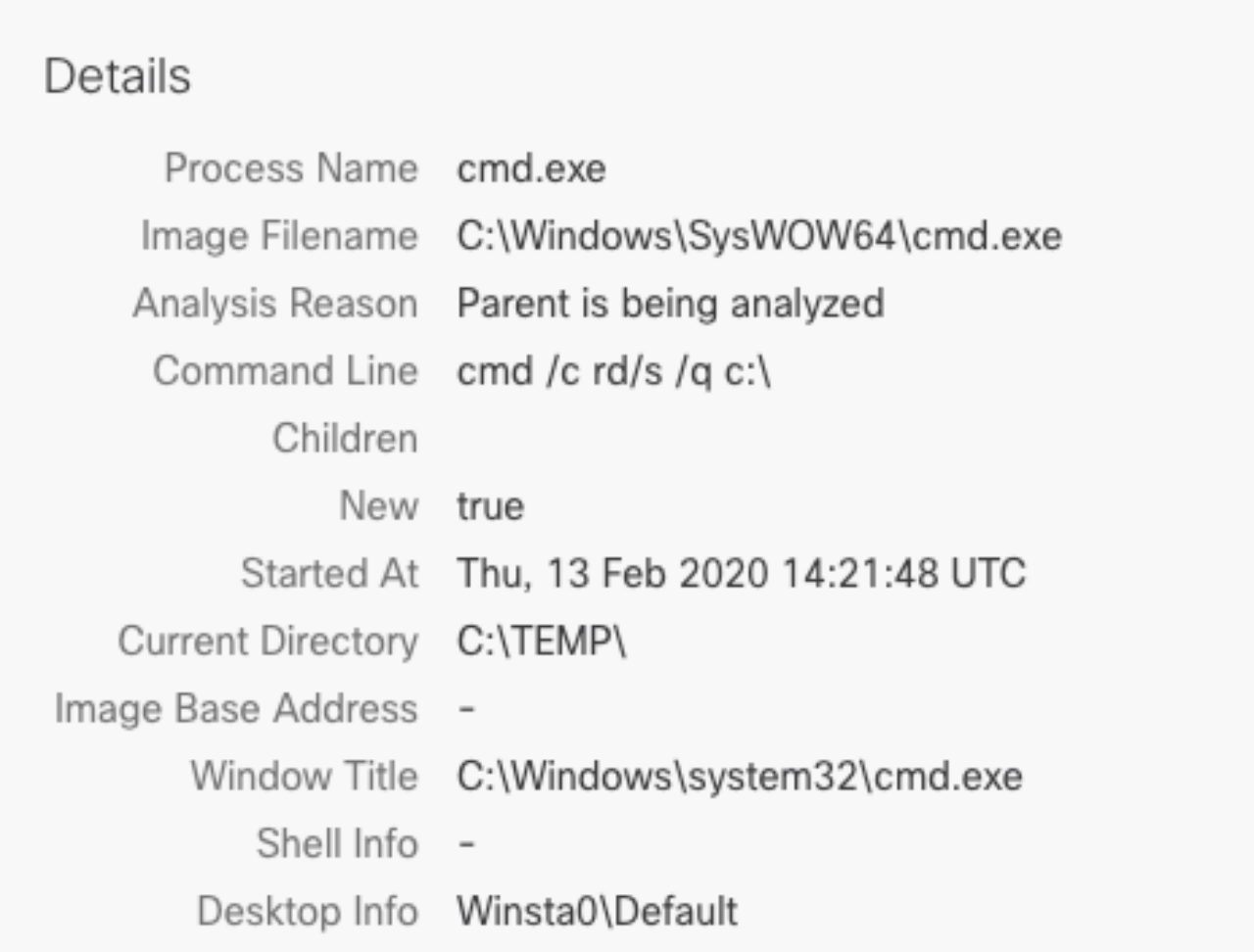
During the course of the investigation, we came across several samples that appeared to be malicious and were tagged as malicious in various engines but were, in fact, odd jokes or non-malicious content, including a fake wiper. This file was found with the suspicious filename of "CoronaVirus.exe" of which there were many. This particular one immediately appeared to lock the screen upon execution.



The rough translation of the text displayed to the user is "Deleting all files and folders on this computer - Coronavirus." Upon completion of the counter, the button at the bottom became clickable, and when clicked, displayed the following message:

This says it is a joke and the user can press Alt + F12 to exit. If the user pushes these buttons, it drops you back at the desktop. Upon further analysis, it does not appear there were any other malicious actions taken. This is just one of several odd examples found in our research including another joke game written in VBS and an odd executable wrapper of a well-known outbreak map for coronavirus. None of these files were malicious but did take actions that could be viewed as malicious, as such, we have seen many antivirus vendors detect these as malicious executables. At the very least, they are unwanted applications, albeit not inherently malicious.

One additional malware sample we discovered was a wiper designed to destroy infected systems. It was initially submitted to various malware repositories with the filename "冠状病毒.exe" which translates to "coronavirus." The malware, when executed on systems, uses several techniques to delete data from both the file system and registry in an attempt to disrupt system operations. For example, we observed the malware invoking the Windows Command Processor and using the "rd" Windows command to iterate through the directory structure of the C:\, deleting the contents:



It is important to note that there is no prior attempt to copy, exfiltrate, or save a copy of the contents and the malware does not appear to make any attempt to extort victims or otherwise generate revenue for the malware author.

Conclusion

Malicious actors are always going to do whatever they can to increase infection rates and in turn increase revenue, this includes using the news and fear to achieve their goals. This is one of the cases where both news and fear can be used. In a world where threats like Emotet are stealing emails and replying in-line users need to be increasingly skeptical of all attachments regardless of source. These attacks can be seen in an email thread with a colleague or friend and, in some cases, may come directly from that colleague or friend. Additionally, anything news related should be treated with a little extra skepticism, go out and do your own research instead of just clicking links and opening documents that are sent your way.

Coverage

Ways our customers can detect and block this threat are listed below.

PRODUCT	PROTECTION
AMP	✔
CloudLock	N/A
CWS	✔
Email Security	✔
Network Security	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of the malware detailed in this post. Below is a screenshot showing how AMP can protect customers from this threat. Try AMP for free here.

Cisco Cloud Web Security (CWS) or Web Security Appliance (WSA) web scanning prevents access to malicious websites and detects malware used in these attacks.

Email Security can block malicious emails sent by threat actors as part of their campaign.

Network Security appliances such as Next-Generation Firewall (NGFW), Next-Generation Intrusion Prevention System (NGIPS), Cisco ISR, and Meraki MX can detect malicious activity associated with this threat.

Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Umbrella, our secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs, and URLs, whether users are on or off the corporate network.

Additional protections with context to your specific environment and threat data are available from the Firepower Management Center.

Open Source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

Indicators of Compromise (IOC)

Hashes (SHA256)

345d8b4c0479d97440926471c2a8bed43162a3d75be12422c1c410f5ec90acd9 (Parallax RAT)
Adde95e8813ca27d88923bd091ca2166553a7b904173ef7a2c04bb3ddf8b14a9 (Wiper)
C57fa2a5d1a65a687f309f23ca3cfc6721d382b06cf894ee5cd01931bbc17a46 (Nanocore)

Emotet Maldocs (SHA256)

006dc4ebf2c47becdc584911627289901477 17a0d9dd76fefa9b7eb83937c60b
0a84308348fee6bbfe64a9ef23bb9c32cb319bcdf5cf78ddfda4a83dadea4b8e
0a8aa3f413a8989bb89599dfc2404f7d34dfbb2e3ce26e900d228e9e8c8908b8
0fdc97da1c297e6fef93910008fc5c47cbdcd3e2987bc163467b34f56de112ff
11b4519b76957b0758381f8e19c5e15d8744f7974716642aeb586c615dde38fa
140da6b610a45f84c6438207ab11942d79eb37831551810f87baae80cfff4593
1c3532d143212078e204d0f81a782deacd58e8f0e7253472e0509491fd1e5201
1e4b01e3e146ff01a3782b01680a5165432af556331d599ec6ad35b4983b216f
2037c7cc809ed3eddd1338d2bec6266cdb449dbf8ff3510fd360a08d229d4f40
21182b7834a7e13033be7b370a68b3d3639f4cae12fe80e2a908404cbd4cd324
2437ef90b60cf3d6bd0c3eebf3f41ed1e403bc31b024b52b0f41ec648d80a583
257afe9f4d7b282b1c0b2f3ebb7e1e80e96c8e0214f1b80ea2b7b636a4e7747d
2bcd35bfb7e4dbdbbf64fce5011199947794425093be7bc74829bfeadb89f0a3
2c9c1e04d806ad8890dd6bf4477efb4ea6c78b8185a9996876bcaea568a04e70
2e47f37bef4dea338e366ce30fe54888e5aaa2d47a5c0db4a3c3e9e5c25f8ace
2f3ee4688a31c8d249b8426f46e392d9c55b85bfad9fb31fb362eb32d38bd9b3
31cb82cd750af6af9ecf369fd26d47dc913f6b56be6ea12b10fe6dd90ef1b5df
32753598f94412fe3dc382dc12dcf2edf7881d9f07814c82aeec36481b9362b5
3386dc7dc67edd5e84244376b6067e3767e914a1cc1fc7fd790a6aa68750a824
37354a04f6d423809602e198e590469173cc8e930cc7fdd4da2c2072977251e9
3981d933de93f55641fdf8cfe980e40a0bf52ce8b022735e8ebc4f08cbb19104
39c17475bdb019010453085830e7f8aa1ef41ca182982491306fcf75166b8e08
3a7a8518b41dd6c05289a08974c95a0038be4e5d1b0588edfd0589fcf22b0c8f
3cd099efe4cb426fdc6276380c224b5478d0841c5c44d2c0a088d039d529d258
3fc33b537fb38e1f586ddb3ebbbe152458dcde336c2f26da81d756e290b5ef00
46f81af256c630969f55554ea832037bc64df4374ec0f06ac83a1c4b89869314
49cfa1b3cbe2bf97079c0dd0a9f604e3f2e7d9fbb6d41128a9889e068aa884f6
4a272dd4a5c6261e983d667dd676875054dd4a4ea11620f16c553fcfd2c44861
501cc107e410b245d1b95b64ae0afdae758375b4b3724acfda44041bad963232
50a3bea4b9686bcf5cac144d4fc18aa178f66c8368205f9065cd1d9a2c41f026
51f0e9b151bde97ebeb813d6eed8a11f02551a6530049f53dc29fc1a20b6699d
587840d28f2585dd5207731d7fda86a0966c82fa592a26f9148b2de45526db55
5b7db5046ba22a6242d5ff6e8f538ad43bba53810117d5eb8f023215aad26e6b
5e20a0ab563950eab76c023101b1dd374becac2a5149a74320b23b59a7f16256
698eb726345c71eca7b4a531bfa76ab6e86ef100f943a727fb5866a84ec79289
6c34cca35d98e464c2f74abd9be670c7f8f707f37cd3f0fd4746c49f8fcf6b07

722a60dfd59a595daa487f2fb759ef6f9ccaabcdf20605d5ae9450cba4a9b9b2
78cf7ea3c1da98941e164f4ac3f75b57e9bce11467bc5a6c6877846f1adcf150
7a97fc7bdd0ad4ef4453c2e52dd8f44dee9b4e91ff3b5518e311ef1ebac3b667
7a9f249978c959e1f11f2992a8ce4a70ba333c8dbdc2638c780bbbe62de4808e
7cbcad4d6e9ad8438e5febd3830bff9aef4729b98d23935ad7f9e6d290272732
7cf8f24d7e8b1e2f63bfa7a18cd420a03fff44126e80aed8cb90fba3c4e986ac
80ee20c604d5d4b51a30dc21da271651f3c085c40281e3ff3e2ee0175d2ca98d
80f8877406e899c6274331aa991b8d1f4f087e3233c36d39fbaebb729c294899
89a0147dec8d6838f14815b577ae41dbcf54953c66e7f5f999ab91fea6ec08fa
8a724fc60bde738694779751d6c63a7ed1caa03518b8f26b9acb36d5c1b29930
8c0a8d6876a6c7fe44962883561d9f48615ee67f4544872ec98f47edcf516509
8f91d27d3a59c08ab4c453b2679f4620696ba67c56280a4c3757368acb20aad3
90c3d8d13ea151bce21a1f4b842d0ed4eaff09842b23311b2326cf63957fc2b2
92af9c8c539ff9f99f79cce8453b1c483d117c095e2e0ffe384d96e35f72dc8b
9367f3ea7460ae40ca69d41398327f97136a93656ef5fad1285a0b82f81522a4
980de93ad93ecaabc048c9fcc9d62e43eeb32f216c4177963cf1bd94ad53074b
9d58ca5383fef5dc837ca9d4251d247bed4ead4a6b90a9aae30568be80e20543
9e4cb963e509fbde6de003a81a3e19cfc703be1c41d20f4b094a0fa89d6ad02c
9f27a826b4b873c9ea23e023f54d5291a50004d67dd5fe64d1f8c8e8b51b74e3
a080d763c60efd4ef2781ad3090c997d1092ac726707366d92d647f26ee2965f
a286e3be694b9525530ec6a65b71a8a91e04042c3471e8a9e440f503fe8ce995
a537c75de9a95be0c071fd6437cbaf3696752f02c3cd5afa1c9cc47c4c755f75
aa6ceb17ced471e1695c99c0718bc24c710311f0daa256cb0783d82218d772c9
ac416780fa4aa340fff2787e630351c5813faceb823424817eb10e82254b785d
b04584ee8b3ba565541cb0f4d8787ed6e8942b6bdec5b1acdc03488b93aeb3cb
b14d70827d5d668aeb31e94be512fea9fb38ead8ec12cdf7617616801c76b6e9
b283e4f841e328f0cc12ebdf76aafb819ebadba7df863681994b69697731cf96
b34f4ec4ae8d66b030f547efe3acc2a71c9ab564f78aac68719ec91dab613bb3
ba4297978b6a6b5fe2b66c32ead47bbd1f2e2f549beed5cd727eb9ae3fed6b6a
bdcef0f16c70086414ff95b69fdbbe7eb0c9814308d3d60143b6c04dfc077257
bf178911f2c063c9592020652dc22076d02ca87d14a7ed7862074d334470ae32
c135f36d3346699e6d2bf9f5f5f638fd9475c0b12144a15a0652b8f1ebb25c12
c6dc408d60c2354a13e835bf826300a6d5258b72b8826e8c46d946cbc1f0b455
c9d3c250ab6d8535b7a4114a1e9545f0b9bc24e4e277640c59b7555f38727885
cba1c3070f76e1a2705afee16bd987b6a8ffa45900cab8cf3b307f60a7b89ac9
cc2507ddd53a6f00265f3be51d7217def786914bd1d700ec3c74a2a7107b3476
d765980228492758a11e534e45924311aef681cb5859f701cd457b6b871c2d06
d8183919d675978d58cd1f134768f88adeea9ce53b167c917e54fff855c6d9f9
da87521ecc146a92a7460a81ebb5ca286450f94c8c9af2a4b3c6c8a180d421c5
dbcef5c217a027b8e29b1b750c42a066650820a129543f19364bcb64ac83bc07
dc66811ce189240c510733be9e1a2175079dddb80ebf02faaa044fce1f7134d0
e17dca7c2c05139fc81302e76e0e9aaa29368b60cb147208cbcb5c8df113f6f6

e250d977e47e7809086dd35a2767f9ef557591dd00e9ce96ef4071e4f0d8c670
e32cca6446f2ddd8430400b16fc171ab3163cf8222669d7d9144e9c85904d5f5
e382ee1ce9d99f4e8e18833bac121c14ee2e5dc29a8b5382ca5b4eda9db7f1aa
e55efa92d87484cf6b251f2302a0c0c7650acd7ea658bf9997bf761b64fe472a
e8221acccdb8381b5da25a1f61f49dda86b861b52fafe54629396ed1e3346282
ea3a0a223474592635d1fb7a0731dd28a96381ad2562e3e064f70e2d4830c39d
eab14b1bfa737644f14f7bb7ace007d418230285364e168e35bd718a6517b316
f2a2bea86ce1a4803345b4aa46824c25d383a0b40b10bb69e528c72305552a2a
f6879431b901df789082452c1c4ffa29e857d247886e421df6dda5fb3d81ca5e
f7209d1099c75acccbef29450271d821fd78ad52176f07aa8a93a9e61e9eaa7f

Domains

vahlallha[.]duckdns[.]org