

[Home](#) / [Blog](#) / [Security Briefs](#) /

Ransomware as an Initial Payload Reemerges: Avaddon, Philadelphia, Mr. Robot, and More

# Ransomware as an Initial Payload Reemerges: Avaddon, Philadelphia, Mr. Robot, and More

**JUNE 25, 2020** | **SHERROD DEGRIPPO**

---

In the past month, Proofpoint researchers have observed a slight increase in email-based ransomware attacks using ransomware as a first-stage payload. This is notable because for the past year or more attackers have used downloaders as the first stage payload, which then deliver ransomware as the second- or later-stage payload. A small increase in the amount of ransomware sent as a first stage payload via email campaigns may herald the return of large ransomware campaigns we saw in 2018.

These attacks have featured many different families of ransomware and have targeted numerous industries in the United States, France, Germany, Greece, and Italy. They often use native language lures and messages. Ransomware families we've seen as first-stage payloads include among others:

- Avaddon (a new family)
- Buran (named for the Russian Space Shuttle)
- Darkgate
- Philadelphia (something previously seen by Proofpoint in 2017)
- Mr. Robot
- Ranion

Each of these ransomware families encrypts the victim's files and holds them ransom for a payment.

themes in these ransomware messages, including some that exploit COVID-19, and numerous industries were targeted. These verticals include education and manufacturing followed by transportation, entertainment, technology, healthcare, and telecommunications.

Below are Avaddon, Mr. Robot, and Philadelphia examples:

### **Avaddon**

Avaddon, a newer ransomware that has targeted U.S. organizations, is notable because it has its own branding and is often part of large-scale campaigns. Over one million messages with Avaddon as the payload were sent June 4-10, 2020, and over 750,000 messages were sent on June 6, 2020 alone. These campaigns were primarily sent to manufacturing, education, media and entertainment organizations. The June 4, 2020 Avaddon campaign focused almost exclusively on transportation companies and school districts.

Avaddon is an example of “ransomware-as-a-service” (RaaS), where threat actors pay others for the use of the ransomware rather than building the ransomware and infrastructure themselves.

Recent Avaddon messages featured subject lines like

- “Do you know him?”
- “Our old picture”
- “Photo for you”
- “Do you like my photo?”
- “Is this you?”
- “Your new photo?”
- “I like this photo”

When opened, the included attachment downloads Avaddon using PowerShell. Once Avaddon runs, it shows the ransom message in Figure 1 and later demands \$800 payment in bitcoin via TOR. The Avaddon attackers also provide 24/7 support and resources on purchasing bitcoin, testing files for decryption and other challenges that may hinder victims from paying the ransom.

RANSOMWARE

Your network has been infected by Avaddon

All your documents, photos, databases and other important files have been encrypted and you are not able to decrypt it by yourself. But don't worry, we can help you to restore all your files!

The only way to restore your files is to buy our special software - Avaddon General Decryptor. Only we can give you this software and only we can restore your files!

You can get more information on our page, which is located in a Tor hidden network.

How to get to our page

- Download Tor browser - https://www.torproject.org/
• Install Tor browser
• Open link in Tor browser - avaddonbotrxmuyl.onion
• Follow the instructions on this page

Your ID:



NDctNzBLTtdFdWZGYXF0SktNZ291TkpxbzVXVDBHMHJRN0tkbk0vOFA4RFVraLV5V2k3eWNORnloZkhWRDgzbGp1U05qNuH2U1FPPO
HJUclVCcUF5L2drVEJqeEhFWXZtRWk0T0FGWnpZMTE2bTBZUiteEQ21TSVRZzG1wOGs4RStpRmN3cXc0NWQ1NG83a2FSaWolaWx1TG
g3dERYQUVueklITVUvTUY3Smd1cEtQN1lBaXE0cUpDc01WeWhjc2FpVmNrRXVjt09kUFUvTHkrTmdsax2Y3lBUFN6Q1B5ZHo4KzI
0RHFGQ3pxY0FKc3YvMkxtU2F3c3BTZVE4VlFVendkRHhmTzNICFBwSWJaQWpoOGt3ZEExCeVduVctayTlyazRoVORUSHNIYk5ObUFz
UkRCYjBmsUVDVzYxzGd6WfLJdnhXandvNXpraU5penB6b0tSZFpVd3BmSHJkenFZeWRWQWRlK3o1RjnNadytSNWREeTJNb0IzblpsZ
VpXsNdYemxRbG80TXgwU53MjzMTTEFCdDlTzjn0eW9CaVZ6UzhSN1Y0aUdvcmtmTGg4Uk14L2JYV1RKV3hhzXVzejRTOWEya3RxUW
h5ZytJSDVPRkpMVE51MEF5MDhiSkczRkliWUFuRmI2MnFrBjRwT1lhSUpvTlUyUUpld0RrL0FBN2NwTW04WmNxmHhIYjFva0s4VC8
zRmtOY3MyK3FmY0VvUGFlchVHZlBWQTNtaUVpZUU3MDk3MVJXadFHMh1hWlRpV3daTXA4aHU3UTlZbHZ0R3grZ3N4ZwZaMLZUSDFo
VkJzRStFQkVDYWNwYwxyL0VIOFdnMnlpSStnWF1lM1BSU2ZPbTgrWWM1RDUyOFNmDM9xzC9QVEVoVXU5WF10OXpmaWJnN0hjejb3S
1hEUW5PcE1hSddhNU9scXurVjzsl0pDVFdHblR3Qlc5VVBURctzV0RYK1UvTnpPWG1iUExMM01jajhXS0tPUGFQWGlASWPNM0nkUX
kxN1hhTUEwZWFkelZQS0huWFBwb2RqQWpJZE5Pvm0xYnlXT2hzSnYzQ1laZGxjcGsyT0oyeHlTSORQRitSeU5WTH12d1VWUGNzWnE
2TnRvc0ttZVhqM1FnLhYvnlWNmdIaFZzQVdQK21QZ1E5WGF0QnkYUNzaVJhUjr1UytBdVRscGd3eXJPSE8yYjc0TRXcDJBMEVr
VmZsSDJhWmtSVmluTXZ2TFA5RURqYS90YXdCekxWQWpjUTFnalJBdEtVnnc4TUpRMGppNwSyadJxc0Z1REE1QU5TRH1IMUVjRDhLe
G1wMldkVcTGS0htNktENFBbCyt3UFdkYnJMqzZMeFRTZi9omUx4bGRqcVZwa3pLVWNwSlJISi9RWkFoRndkdDJySFGZE9EKy9Ial
1kTmFhdktlZjz0aJroU05ObU9tZzFxeDgxWXpIL1N4NkVqahZFMGJqu1VwZ1grUUtPdmZrRnpLZEZFV0xTV2tmd1E4Y1NuYvhpMVA
rV3lUTURBOH12NWNwSFJtQkNUTkxsbDVhTnhncFVRMlZQY1V2dEF1LzBROVZJdDd6ZTFoeUFubVgxdEVDc0FLZkdzVE1DU1hTdktr
SkVQWRWrdUxCVstAn2xacGJtdDBrYlFKbnpTZ2YrSnhzRVFPm4zamNkTENCnjzicHEwRnFmcUpwWw93K1ZwQTFfckZ1a1M2UnRXZ
3EvYmw2YlJZRjk5VD1FbjZyCmxqUmpa3BzOVRMcFROQ3FoUzNDRNjyYTNFSEIwdHpUOTBzb3BJeWFBVeVRWbEovTGEwdGFqWk9RaH
Bld0tuL2xGMHhPV2NpVzhqSUNVTktyaja0Lz1YRGg2Vm00mj1KTFMrduXyde8yYw==

DO NOT TRY TO RECOVER FILES YOURSELF!
DO NOT MODIFY ENCRYPTED FILES!
OTHERWISE, YOU MAY LOSE ALL YOUR FILES FOREVER!

Figure 1 Avaddon Infection Message

Mr. Robot

This Mr. Robot ransomware attack used a COVID-19 lure to persuade targeted users to click. Between May 19-June 1, 2020, a series of Mr. Robot campaigns targeted U.S. entertainment, manufacturing, and construction organizations.

Recipients of these campaigns are sent messages claiming to be from "Departament (sic) of health", "Departament (sic) of health & human services", "Health Service", and "Health Care" with subject lines like:

- Your COVID\_19 results # 99846
- View your COVID19 result # 99803
- human immunodeficiency virus analysis # 93545
- COVID19 virus test result / 61043
- COVID19 virus result / 64745
- COVID19 virus analysis # 83273
- Check your COVID\_19 test # 65619
- Your COVID\_19 Results No 80420

The recipient is encouraged to click a link in the message as shown in Figure 2. If clicked, Mr. Robot ransomware installs, and a \$100 payment demand appears.

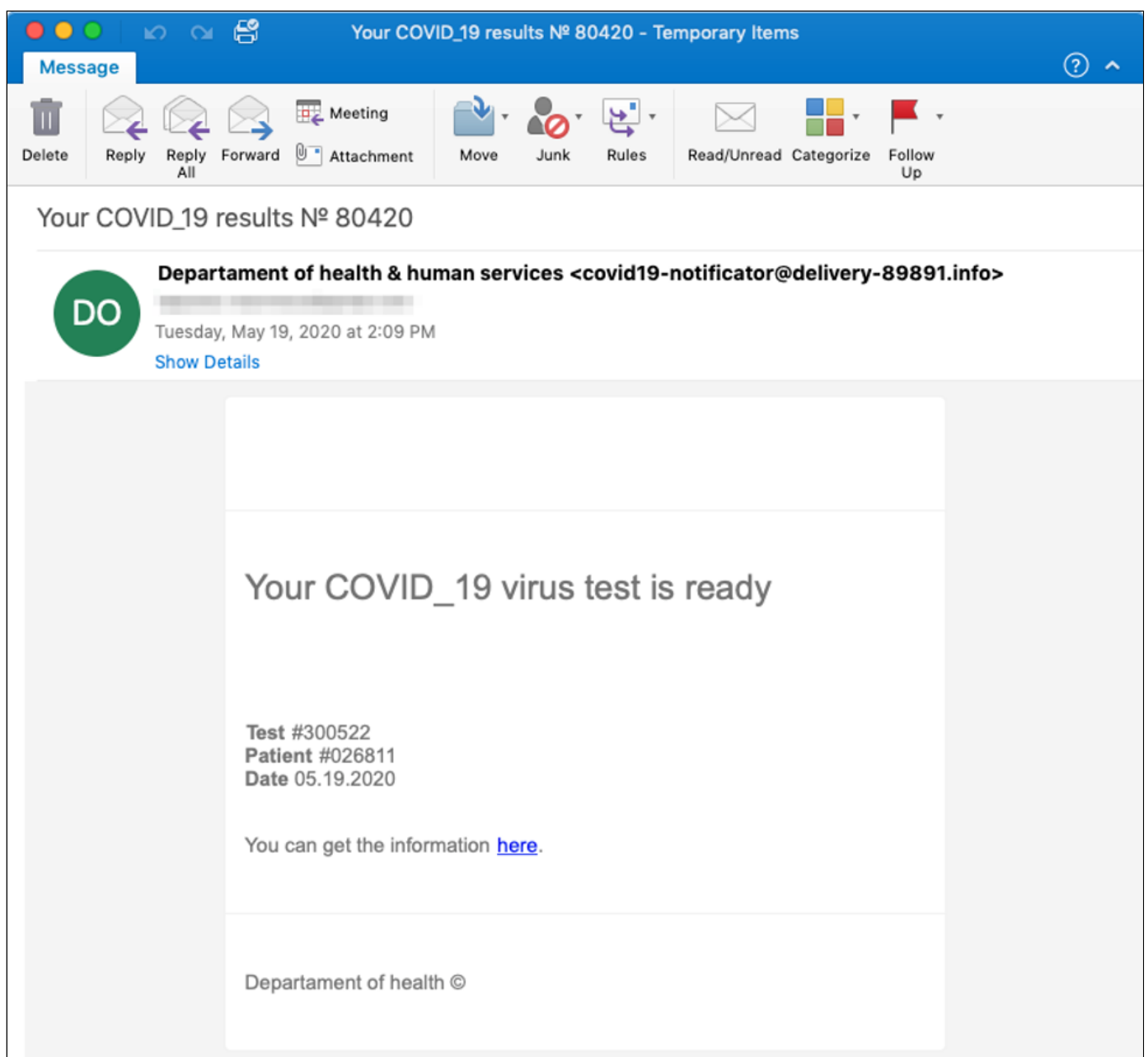


Figure 2 Mr. Robot COVID-19 Lure

lures (Figure 3).


These messages claim to come from “Federal Germany Government” and use the flag and insignia of the Federal Republic of Germany, along with a subject that states: “Die Entscheidung, Ihr Unternehmen aufgrund von Covid-19 zu schließen” (translated: “The decision to close your company due to Covid-19”). The recipient is encouraged to click the link which installs Philadelphia as a first-stage payload and shows a ransom message demanding (in English) payment of 200 Euros as shown in Figure 4.

From: Federal Germany Government <state@germany-government.eu> ☆

Subject: Die Entscheidung, Ihr Unternehmen aufgrund von Covid-19 zu schließen

To: [REDACTED]

06/06/2020 à 13:26



Federal Republic of Germany  
The Federal Government

**Die Entscheidung, Ihr Unternehmen aufgrund von Covid-19 zu schließen**

Aufgrund der aktuellen Bedingungen unseres Landes aufgrund von Covid-19 haben wir beobachtet und berichtet, dass Ihr Unternehmen die Bedingungen nicht erfüllt.

Bitte schließen Sie Ihr Unternehmen innerhalb von 48 Stunden und öffnen Sie es erst, wenn wir Sie erneut anweisen. Andernfalls werden Sie für einen hohen Betrag verurteilt und mit einer Geldstrafe belegt.

Ein Dokument, aus dem hervorgeht, dass Ihr Arbeitsplatz von unserem Expertenteam nicht geeignet ist, ist beigefügt.

**Beachtung! Da das angehängte Dokument für Sie bestimmt ist, lassen Sie bitte alle Antivirenprogramme und Windows Defender, falls verfügbar.**

**Andernfalls können Sie das Dokument nicht anzeigen.**

- Schützen Sie sich und andere um Sie herum, indem Sie die Fakten kennen und geeignete Vorsichtsmaßnahmen treffen. Befolgen Sie die Anweisungen Ihres örtlichen Gesundheitsamtes:
  - Um die Ausbreitung von COVID-19 zu verhindern:
    - Reinigen Sie Ihre Hände oft. Verwenden Sie Seife und Wasser oder eine Handmassage auf Alkoholbasis.
    - Halten Sie einen Sicherheitsabstand zu Personen ein, die husten oder niesen.
      - Berühren Sie nicht Ihre Augen, Nase oder Mund.
    - Bedecken Sie Nase und Mund mit Ihrem gebogenen Ellbogen oder einem Papiertaschentuch, wenn Sie husten oder niesen.
      - Bleib zu Hause, wenn du dich unwohl fühlst.
    - Wenn Sie Fieber, Husten und Atembeschwerden haben, suchen Sie einen Arzt auf. Rufen Sie im Voraus an.
      - Befolgen Sie die Anweisungen Ihrer örtlichen Gesundheitsbehörde.
  - Durch die Vermeidung unnötiger Besuche in medizinischen Einrichtungen können Gesundheitssysteme effektiver arbeiten und Sie und andere schützen.

**Dokumente herunterladen**






Figure 3 Philadelphia German Lure

```
All your documents (databases, texts, images, videos, musics etc.) were encrypted. The encryption was done using a secret key that is now on our servers.  
  
To decrypt your files you will need to buy the secret key from us. We are the only on the world who can provide this for you.  
  
What can I do?  
  
Pay the ransom, in bitcoins, in the amount and wallet below. You can use LocalBitcoins.com to buy bitcoins.  
  
Send BTC 0,023 = 200 EURO  
  
BTC Address == 1NxoWvpXufC5PkagnfWD9Rf19wm5jchVkX
```

Figure 4 Philadelphia Ransom Note

This recent emergence of ransomware as an initial payload is unexpected after such a long, relatively quiet period. The change in tactics could be an indicator that threat actors are returning to ransomware and using it with new lures. Various actors trying ransomware payloads as the first stage in email has not been seen in significant volumes since 2018. While these volumes are still comparatively small, this change is noteworthy. The full significance of this shift isn't yet clear, what is clear is that the threat landscape is changing rapidly, and defenders should continue to expect the unexpected.

About

Threat Center

Overview

Latest Threat Report

Why Proofpoint

Human Factor Report

Careers

Threat Glossary

Leadership Team

Threat Blog

News Center

Daily Ruleset

Investors Center

Email Protection

Advanced Threat Protection

Security Awareness Training

Cloud Security

Archive & Compliance

Information Protection

Digital Risk Protection

Product Bundles

Nexus Platform

Whitepapers

Webinars

Datasheets

Events

Customer Stories

Blog

Free Trial

### Connect

**+1-408-517-4710**

Contact Us

Office Locations

Request a Demo

### Support

Support Login

Support Services

IP Address Blocked?



© 2020. All rights reserved.

[Terms and conditions](#)

[Privacy Policy](#)

[Sitemap](#)