TA2101 plays government imposter to distribute malware to German, Italian, and US organizations

proofpoint.com/us/threat-insight/post/ta2101-plays-government-imposter-distribute-malware-german-italian-and-us

November 14, 2019

Blog

Threat Insight

TA2101 plays government imposter to distribute malware to German, Italian, and US organizations

November 14, 2019 Bryan Campbell and the Proofpoint Threat Insight Team

Overview

Proofpoint researchers recently detected campaigns from a relatively new actor, tracked internally as TA2101, targeting German companies and organizations to deliver and install backdoor malware.

The actor initiated their campaigns impersonating the *Bundeszentralamt fur Steuern*, the German Federal Ministry of Finance, with lookalike domains, verbiage, and stolen branding in the emails.

For their campaigns in Germany, the actor chose Cobalt Strike, a commercially licensed software tool that is generally used for penetration testing and emulates the type of backdoor framework used by Metasploit, a similar penetration testing tool.

The product describes itself as “adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors,” and is intended for use by organizations to secure their environments. However, despite its extensive legitimate use as a simulation tool, various actors have deployed and executed campaigns using it as actual malware, including Cobalt Group, APT32, and APT19.

Proofpoint researchers have also observed this actor distributing Maze ransomware, employing similar social engineering techniques to those it uses for Cobalt Strike, while also targeting organizations in Italy and impersonating the *Agenzia Delle Entrate*, the Italian Revenue Agency. We have also recently observed the actor targeting organizations in the United States using the IcedID banking Trojan while impersonating the United States Postal Service (USPS)

Campaigns

Between October 16 and November 12, 2019, Proofpoint researchers observed the actor sending malicious email messages to organizations in Germany, Italy, and the United States, targeting no particular vertical but with recipients that were heavily weighted towards business and IT services, manufacturing, and healthcare.

October 16 and 23, 2019

On October 16 and 23, Proofpoint researchers observed hundreds of emails attempting to deliver malicious Microsoft Word attachments with German lures impersonating the *Bundeszentralamt fur Steuern*, the German Federal Ministry of Finance. Of particular note is the use of stolen branding as well as the use of lookalike **.icu** domains used for the sender email address in order to craft effective lures.

The lure states that a 2019 tax refund is due ("*Benachrichtigung über die Steuerrückerstattung"*) based on prior returns in the amount of several hundred euros (€694.00 in the observed sample) and that the recipient should submit a refund request (using an attached Microsoft Word document form) within three days for processing. The emails, as part of a low-volume campaign, were targeted primarily at IT services companies.

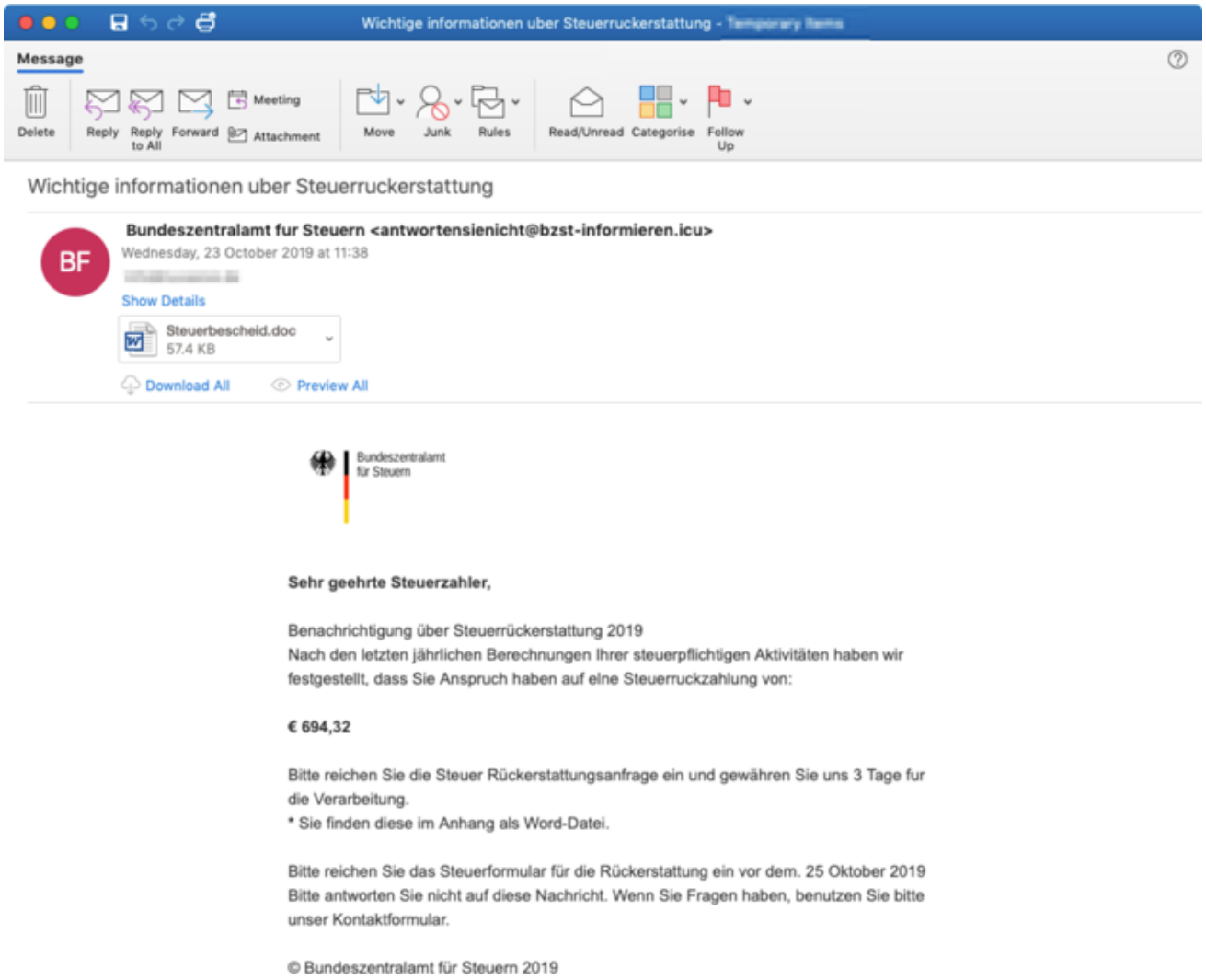


Figure 1: Email lure sent on October 23, purporting to be from the German Federal Ministry of Finance, notifying the recipient of a tax refund, with a malicious Microsoft Word attachment.

The Microsoft Word attachment, when opened, executes a Microsoft Office macro that, in turn, executes a PowerShell script, which downloads and installs the Maze ransomware payload onto the victim's system.

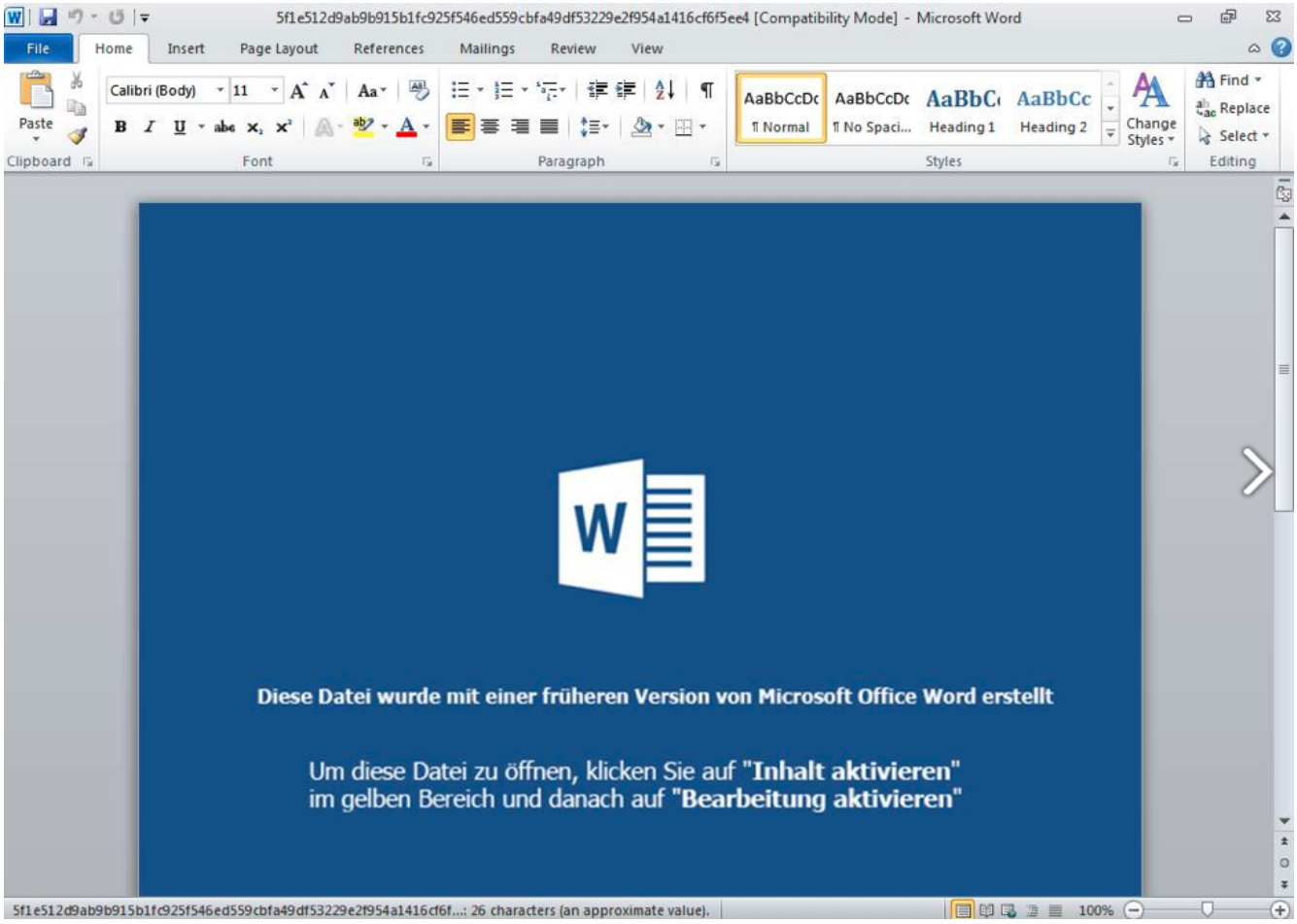


Figure 2: A German-language malicious Microsoft Word Attachment that — if the user enables macros — executes a Microsoft Office macro that in turn runs a PowerShell script that downloads Cobalt Strike.

October 29, 2019

On October 29, Proofpoint researchers observed dozens of emails attempting to deliver malicious Microsoft Word attachments with Italian lures impersonating the *Agenzia Entrate*, the Italian Ministry of Taxation. As with the initially observed German campaign, the actor has used stolen branding as well as lookalike**.icu** domains used for the sender email address in order to craft effective lures.

The lure appears to be a notification of law enforcement activities ("*aggiornamento: attivita di contrasto all'evasione*") and states that the recipient should open and read the enclosed document in order to avoid further tax assessment and penalties.

The emails, as part of a low-volume campaign across multiple verticals, were targeted primarily at manufacturing companies and used an infection chain of Microsoft Office macros into a PowerShell script, which ultimately downloads and installs Maze ransomware.

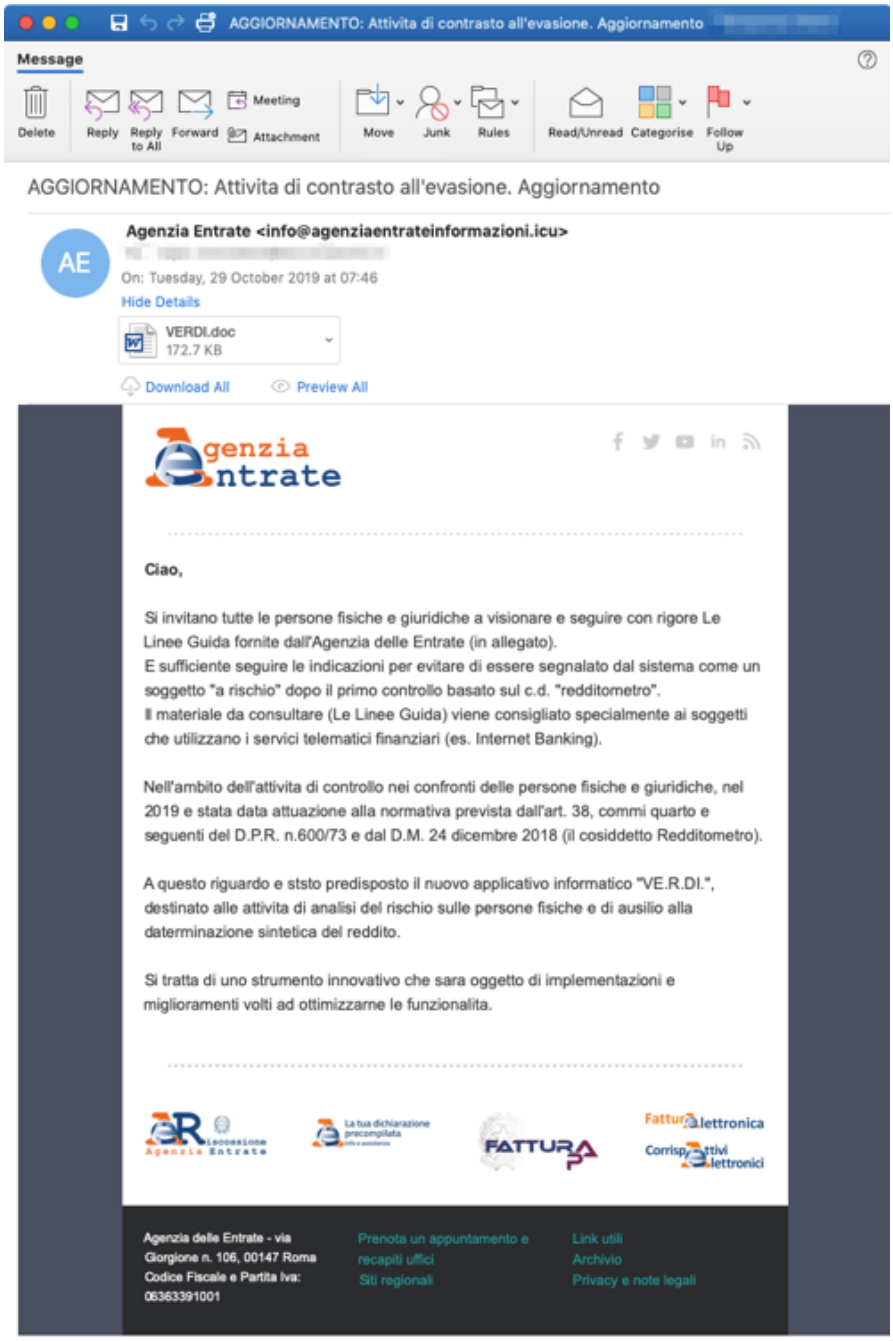


Figure 3: The email lure sent to Italian organizations is a notification of law enforcement activities, urging the recipient to open and read the enclosed document in order to avoid further tax assessment and penalties.

The malicious document purports to be an RSA SecurID key used by the Italian Ministry of Taxation.

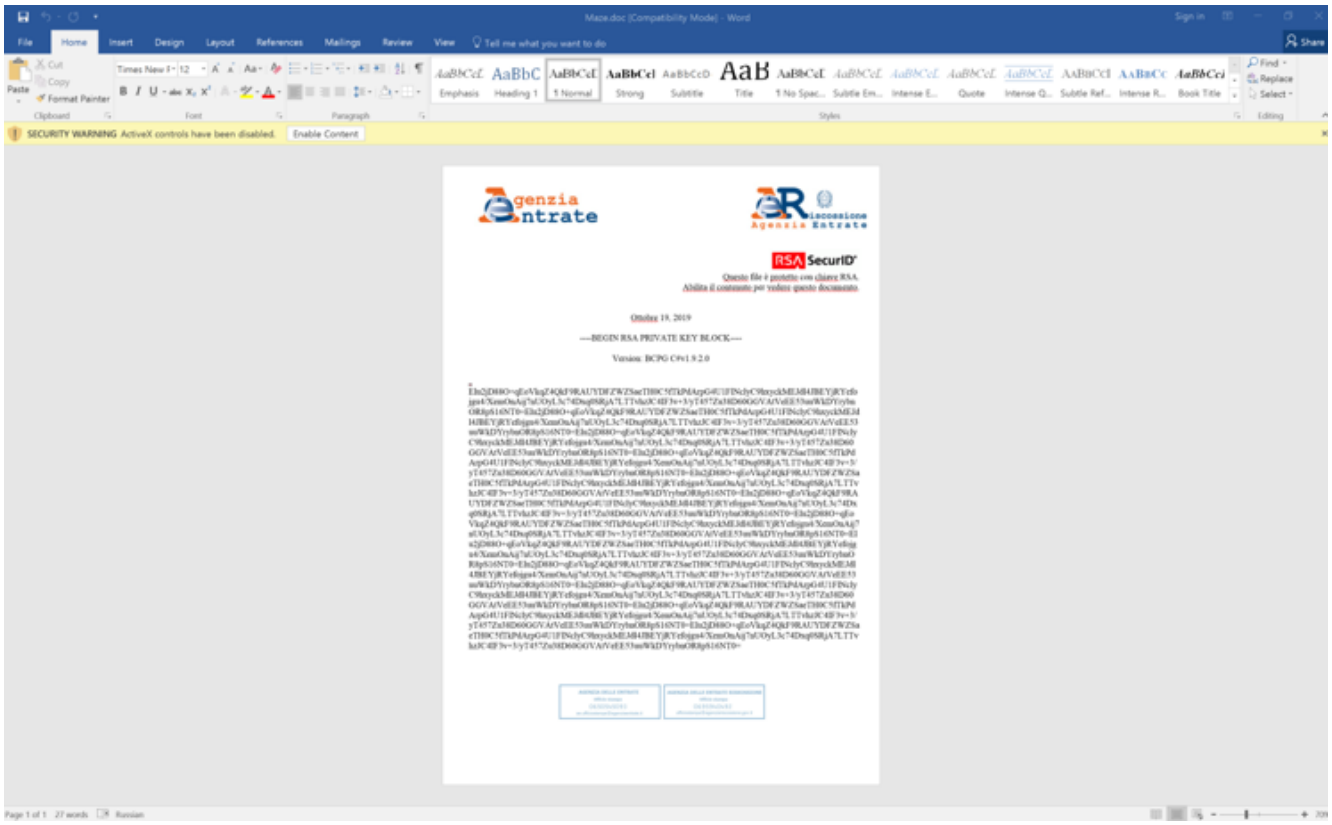


Figure 4: A Microsoft Word attachment in the Italian language, when opened and the user enables macros, executes a Microsoft Office macro that runs a PowerShell script, which in turn downloads and installs the Maze ransomware payload onto the victim's system.

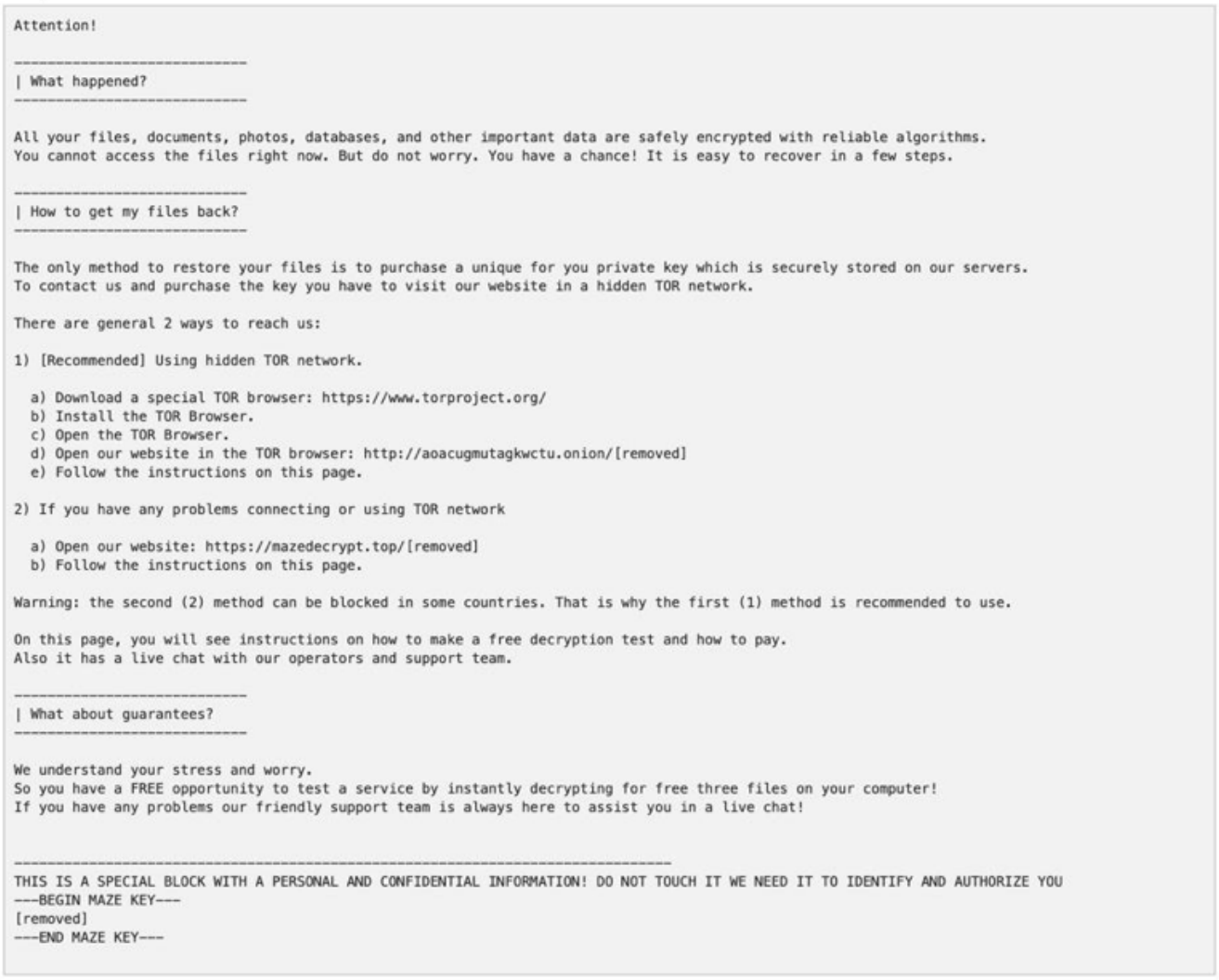
November 6, 2019

On November 6, 2019, Proofpoint researchers observed hundreds of emails attempting to deliver malicious Microsoft Word attachments with German lures, again impersonating the German Federal Ministry of Finance. As with the previous two campaigns, the actor used stolen branding as well as the use of lookalike **.icu** domains used for the sender email address in order to craft effective lures. The malicious document purports to be an RSA SecurID key used by the German Ministry of Finance.

The emails, as part of a low-volume campaign, were targeted primarily at business and IT services companies and used the same infection chain outlined for previous campaigns.

Figure 5: A German-language Microsoft Word attachment which, when opened and the user enables macros, executes a Microsoft Office macro that runs a PowerShell script, which in turn downloads and installs the Maze ransomware payload onto the victim's system.

Opening the Microsoft Word Document and enabling macros installs Maze ransomware on the user's system, encrypting all of their files, and saves a ransom note resembling the following in TXT format in every directory.



```
Attention!

------------------------------
| What happened?
------------------------------

All your files, documents, photos, databases, and other important data are safely encrypted with reliable algorithms.
You cannot access the files right now. But do not worry. You have a chance! It is easy to recover in a few steps.

------------------------------
| How to get my files back?
------------------------------

The only method to restore your files is to purchase a unique for you private key which is securely stored on our servers.
To contact us and purchase the key you have to visit our website in a hidden TOR network.

There are general 2 ways to reach us:

1) [Recommended] Using hidden TOR network.

  a) Download a special TOR browser: https://www.torproject.org/
  b) Install the TOR Browser.
  c) Open the TOR Browser.
  d) Open our website in the TOR browser: http://aoacugmutagkwctu.onion/[removed]
  e) Follow the instructions on this page.

2) If you have any problems connecting or using TOR network

  a) Open our website: https://mazedecrypt.top/[removed]
  b) Follow the instructions on this page.

Warning: the second (2) method can be blocked in some countries. That is why the first (1) method is recommended to use.

On this page, you will see instructions on how to make a free decryption test and how to pay.
Also it has a live chat with our operators and support team.

------------------------------
| What about guarantees?
------------------------------

We understand your stress and worry.
So you have a FREE opportunity to test a service by instantly decrypting for free three files on your computer!
If you have any problems our friendly support team is always here to assist you in a live chat!


--------------------------------------------------------------------------------
THIS IS A SPECIAL BLOCK WITH A PERSONAL AND CONFIDENTIAL INFORMATION! DO NOT TOUCH IT WE NEED IT TO IDENTIFY AND AUTHORIZE YOU
---BEGIN MAZE KEY---
[removed]
---END MAZE KEY---
```

Figure 6: Example ransom notice stored on a victim's system after their files have been encrypted by Maze ransomware.

November 7, 2019

On November 7, 2019, Proofpoint researchers observed hundreds of emails attempting to deliver malicious Microsoft Word attachments with German lures, this time impersonating a German internet service provider, 1&1 Internet AG.

As with the November 6 campaigns, the actor employed the use of lookalike **.icu** domains used for the sender email address in order to craft effective lures. The campaign was accompanied by a malicious Microsoft Word attachment with a purported RSA SecurID key, similarly-formatted to the one used in the November 6 campaign.

1&1 Internet AG
Elgendorfer Strabe 57
56410 Montabaur
E-mail. info@1und1.de
Kopie E-Mail. support@hosting.1und1.de
Kopie E-Mail. rechnungsstelle@1und1.de
Fax. 0721 / 91374226

KdNr.: 19340003422

RSA SecurID

Diese Datei ist durch den RSA-Schlüssel geschützt.
Um diese Datei zu öffnen, klicken Sie auf "Inhalt aktivieren"
im gelben Bereich und danach auf "Bearbeitung aktivieren"

November 7, 2019

----BEGIN RSA PRIVATE KEY BLOCK----

Version: BCPG C#v1.9.2.0

Elu2jD88O+qEoVkqZ4QkF9RAUYDFZWZSaeTH0C5fTkPdArpG4U1FlNclyC9hxyckMEJdl4JBEYjRYefoj
gu4/XemOnAij7nUOyL3c74Dxq0SRjA7LTTvhzJC4IF3v+3/yT457Zu38D60GGVAtVeEE53uuWkDYrybnO
R8pS16NT0=Elu2jD88O+qEoVkqZ4QkF9RAUYDFZWZSaeTH0C5fTkPdArpG4U1FlNclyC9hxyckMEJdl
4JBEYjRYefojgu4/XemOnAij7nUOyL3c74Dxq0SRjA7LTTvhzJC4IF3v+3/yT457Zu38D60GGVAtVeEE53u
uWkDYrybnOR8pS16NT0=Elu2jD88O+qEoVkqZ4QkF9RAUYDFZWZSaeTH0C5fTkPdArpG4U1FlNclyC
9hxyckMEJdl4JBEYjRYefojgu4/XemOnAij7nUOyL3c74Dxq0SRjA7LTTvhzJC4IF3v+3/yT457Zu38D60GG
VAtVeEE53uuWkDYrybnOR8pS16NT0=Elu2jD88O+qEoVkqZ4QkF9RAUYDFZWZSaeTH0C5fTkPdArp
G4U1FlNclyC9hxyckMEJdl4JBEYjRYefojgu4/XemOnAij7nUOyL3c74Dxq0SRjA7LTTvhzJC4IF3v+3/yT45
7Zu38D60GGVAtVeEE53uuWkDYrybnOR8pS16NT0=Elu2jD88O+qEoVkqZ4QkF9RAUYDFZWZSaeTH0
C5fTkPdArpG4U1FlNclyC9hxyckMEJdl4JBEYjRYefojgu4/XemOnAij7nUOyL3c74Dxq0SRjA7LTTvhzJC4
IF3v+3/yT457Zu38D60GGVAtVeEE53uuWkDYrybnOR8pS16NT0=Elu2jD88O+qEoVkqZ4QkF9RAUYDF
ZWZSaeTH0C5fTkPdArpG4U1FlNclyC9hxyckMEJdl4JBEYjRYefojgu4/XemOnAij7nUOyL3c74Dxq0SRj
A7LTTvhzJC4IF3v+3/yT457Zu38D60GGVAtVeEE53uuWkDYrybnOR8pS16NT0=Elu2jD88O+qEoVkqZ4
QkF9RAUYDFZWZSaeTH0C5fTkPdArpG4U1FlNclyC9hxyckMEJdl4JBEYjRYefojgu4/XemOnAij7nUOy
L3c74Dxq0SRjA7LTTvhzJC4IF3v+3/yT457Zu38D60GGVAtVeEE53uuWkDYrybnOR8pS16NT0=Elu2jD88
O+qEoVkqZ4QkF9RAUYDFZWZSaeTH0C5fTkPdArpG4U1FlNclyC9hxyckMEJdl4JBEYjRYefojgu4/Xem
OnAij7nUOyL3c74Dxq0SRjA7LTTvhzJC4IF3v+3/yT457Zu38D60GGVAtVeEE53uuWkDYrybnOR8pS16N
T0=Elu2jD88O+qEoVkqZ4QkF9RAUYDFZWZSaeTH0C5fTkPdArpG4U1FlNclyC9hxyckMEJdl4JBEYjR
Yefojgu4/XemOnAij7nUOyL3c74Dxq0SRjA7LTTvhzJC4IF3v+3/yT457Zu38D60GGVAtVeEE53uuWkDYr
ybnOR8pS16NT0=Elu2jD88O+qEoVkqZ4QkF9RAUYDFZWZSaeTH0C5fTkPdArpG4U1FlNclyC9hxyckM
EJdl4JBEYjRYefojgu4/XemOnAij7nUOyL3c74Dxq0SRjA7LTTvhzJC4IF3v+3/yT457Zu38D60GGVAtVeEE
53uuWkDYrybnOR8pS16NT0=Elu2jD88O+qEoVkqZ4QkF9RAUYDFZWZSaeTH0C5fTkPdArpG4U1FlNc
lyC9hxyckMEJdl4JBEYjRYefojgu4/XemOnAij7nUOyL3c74Dxq0SRjA7LTTvhzJC4IF3v+3/yT457Zu38D60
GGVAtVeEE53uuWkDYrybnOR8pS16NT0=Elu2jD88O+qEoVkqZ4QkF9RAUYDFZWZSaeTH0C5fTkPdA
rpG4U1FlNclyC9hxyckMEJdl4JBEYjRYefojgu4/XemOnAij7nUOyL3c74Dxq0SRjA7LTTvhzJC4IF3v+3/yT
457Zu38D60GGVAtVeEE53uuWkDYrybnOR8pS16NT0=

Figure 7: A German-language Microsoft Word attachment which, when opened and the user enables macros, executes a Microsoft Office macro that launches a PowerShell script, in turn, which downloads and installs the Maze ransomware payload onto the victim's system.

The emails, as part of a low-volume campaign, were targeted primarily at business and IT services companies, using the same infection chain.

November 12, 2019

On November 12, 2019, Proofpoint researchers observed thousands of emails attempting to deliver malicious Microsoft Word attachments with English lures, this time impersonating the United States Postal Service (USPS) and distributing the IcedID banking Trojan.

The campaign differed from previous European campaigns in that the actor chose a **.com** lookalike, **uspsdelivery-service.com** instead of a **.icu** domain. The campaign was accompanied by a malicious Microsoft Word attachment with a purported RSA SecurID key, similarly-formatted to the one used in the previous campaigns.

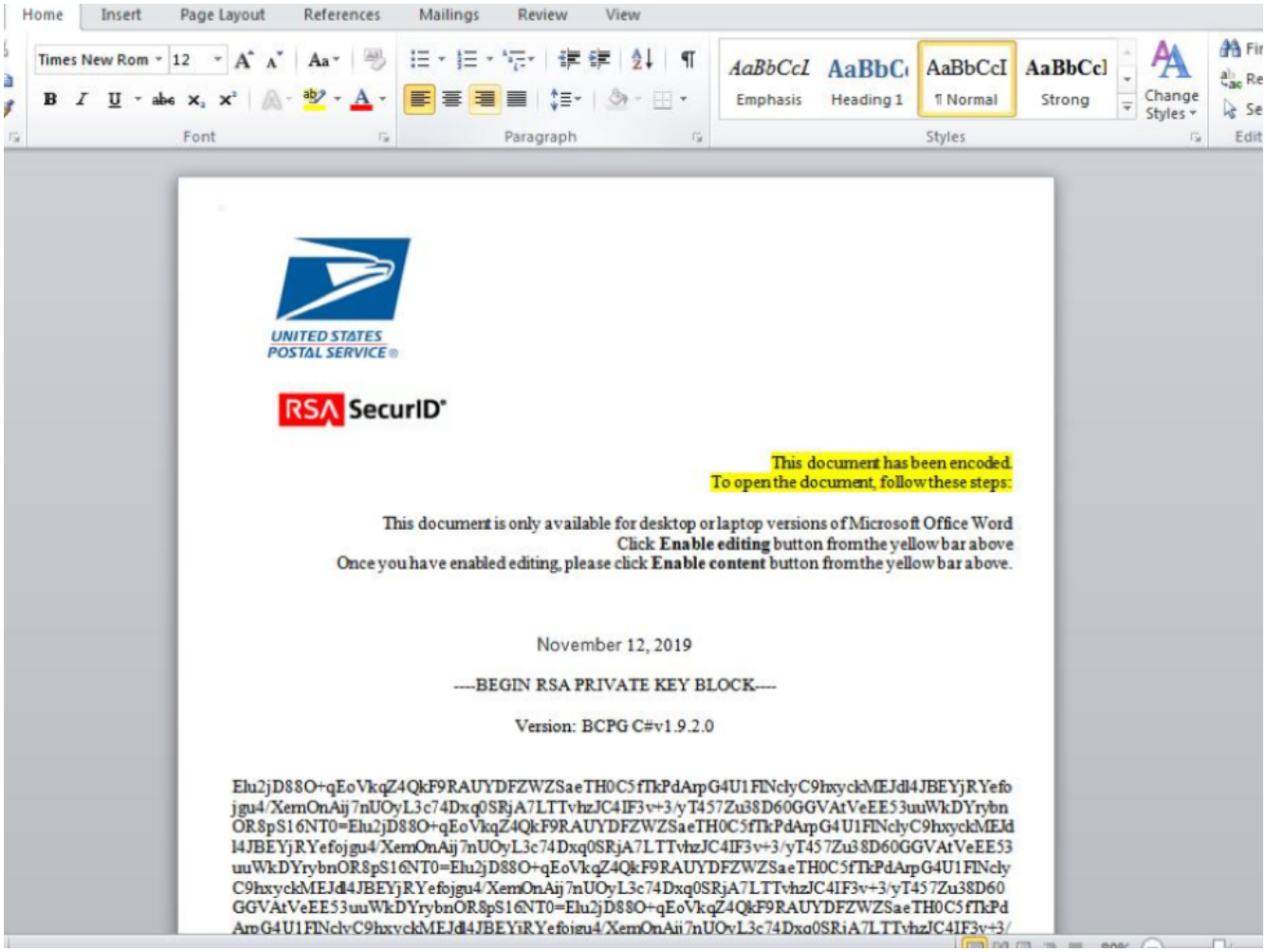


Figure 8: An English-language Microsoft Word attachment which, when opened and the user enables macros, executes a Microsoft Office macro that launches a PowerShell script, which in turn downloads and installs the IcedID payload onto the victim's system.

The emails, as part of a medium-volume campaign, were targeted heavily at the Healthcare vertical, using the same infection chain.

Domain and URL Analysis

Proofpoint researchers have observed a consistent set of TTPs (Tactics, Techniques, and Procedures) that allows attribution of these campaigns to a single actor with high confidence. These include the use of **.icu** domains, as well as identical email addresses for the Start of Authority (SOA) resource records stored for the DNS entries for the domains used in these campaigns.

Additionally, Proofpoint researchers have observed that the canonical URLs used by this actor are formatted in a repeatable fashion with **word_/.tmp** in the string with slight variations made over time (included in the IOC section below.) Proofpoint researchers suspect that the **word_/.tmp** usage might be linked to previous campaigns that were spotted earlier by the infosec community in 2019.

The connection between **gladkoff1991@yandex.ru** extends beyond the more recent Cobalt Strike campaigns, with references to SOA records from September 2019 “eFax” themed Buran Ransomware campaigns.

German Cobalt Strike/German Tax Office spoof (October 23)

Lure email address: **antwortensienicht@bzst-informieren.icu**

SOA: **gladkoff1991@yandex.ru**

Italian Maze Campaign/Italian Ministry of Taxation spoof (October 29)

Lure email address: **info@agenziaentrate.icu**

SOA: **gladkoff1991@yandex.ru**

Proofpoint researchers have also determined that the IP address **91.218.114[.]37** is present in all Maze Ransomware downloads initiated by this actor.

German Maze Campaign/German Tax Office spoof (November 6)

This campaign uses an identical lure that was observed on October 23, including the same "RSA Key" malicious Microsoft Word attachment. It is also where we observed the second use of **word_/.tmp** variation on the URL.

German Maze Campaign/German ISP spoof (November 7)

This campaign, distributing Maze ransomware, impersonates a German internet service provider (1&1 Internet AG) and uses a nearly identical malicious Word Document with an "RSA Key" lure that was observed in the November 6 German Tax Office campaign and the October 23 German campaign using Cobalt Strike.

Lure email address: **antwortensienicht@bzstinform.icu**

SOA: **gladkoff1991@yandex.ru**, which matches the October 23 Cobalt Strike campaign.

US IcedID Campaign / USPS Spoof (November 12)

On November 12, Proofpoint researchers observed a campaign utilizing a USPS themed lure delivering the IcedID Trojan. While a **.icu** domain was not used in this campaign, instead choosing a different look-alike domain, **uspsdelivery-service[.]com**, these malicious documents used similar “RSA” style lures

observed in the previous Cobalt Strike and Maze Ransomware campaigns, and added further evidence to support the theory that the same actor/group is behind the distribution of those malware families.

The SOA for **uspsdelivery-service[.]com** is **gladkoff1991@yandex.ru** which matches previous campaigns.

Conclusion

As detailed in Proofpoint's April 2019 Threat Insight post, Tax-themed Email Campaigns Target 2019 Filers, finance-related lures have been used seasonally with upticks in tax-related malware and phishing campaigns leading up to the annual tax filing deadlines in different geographies. In 2017, these campaigns focused on phishing and increasingly sophisticated social engineering, as well as banking Trojans and ransomware. In 2018, Proofpoint researchers continued to observe sophisticated email campaigns that featured urgent tax-themed lures and convincing spoofs of IRS branding in the United States.

With these new campaigns launched in Germany and Italy utilizing similar urgent tax-assessment and refund lures, Proofpoint researchers have now observed similar spoofs in Europe distributing backdoor Trojans such as Cobalt Strike as well as Maze ransomware. These email spoofs are notable for using convincing stolen branding and lookalike domains of European taxation agencies and other public-facing entities such as Internet service providers. Most recently, the actor has attacked US organizations spoofing the United States Postal Service. The increasing sophistication of these lures mirrors improved social engineering and a focus on effectiveness over quantity appearing in many campaigns globally across the email threat landscape.

References

[1] https://www.bromium.com/buran-ransomware-targets-german-organisations-through-malicious-spam-campaign/

Indicators of Compromise (IOCs)

IOC	IOC Type	Description
44991186a56b0d86581f2b9cc915e3af426a322d5c4f43a984e6ea38b81b7bed	SHA256	Document
cfd8e3a47036c4eeeb318117c0c23e126aea95d1774dae37d5b6c3de02bdfc2a	SHA256	Document
9f2139cc7c3fad7f133c26015ed3310981de26d7f1481355806f430f9c97e639	SHA256	Document
5f1e512d9ab9b915b1fc925f546ed559cbfa49df53229e2f954a1416cf6f5ee4	SHA256	Document
97043f23defd510607ff43201bb03b9916a23bd71b5bdf97db357e5026732506	SHA256	Document

d617fd4b2d0824e1a7eb9693c6ec6e71447d501d24653a8e99face12136491a8	SHA256	Document
7e3ab96d2628e0a9970802b47d0356dc9b99994d7f98492d4e70a5384891695a	SHA256	Document
antowortensienicht@bzst-infomieren[.]icu	Domain	Spoofed sending domain
info@agenziaentrate[.]icu	Domain	Spoofed sending domain
antwortensienicht@bzstinform[.]icu	Domain	Spoofed sending domain
uspsdelivery-service[.[com	Domain	Spoofed sending domain
hxxp://198.50.168.67/wordpack.tmp	Payload	Cobalt Strike
hxxp://conbase.top/sys.bat	Payload	Cobalt Strike
hxxp://104.168.198.208/wordupd.tmp	Payload	Maze Ransomware
hxxp://104.168.215.54/wordupd.tmp	Payload	Maze Ransomware
hxxp://104.168.174.32/wordupd_3.0.1.tmp	Payload	Maze Ransomware
hxxp://192.119.68.225/wordupd1.tmp	Payload	Buran Ransomware
hxxp://108.174.199.10/wordupd3.tmp	Payload	Buran Ransomware
hxxp://54.39.233.175/wupd19823.tmp	Payload	Buran Ransomware
hxxp://54.39.233.131/word1.tmp	Payload	Buran Ransomware

hxxp://104.168.198.230/wordupd.tmp	Payload	IcedID

ET and ETPRO Suricata/Snort Signatures

ETPRO TROJAN W32.HTTP.Stager Checkin M1

ET TROJAN Possible Maze Ransomware Activity

ET TROJAN Observed Buran Ransomware UA (BURAN)

ET TROJAN Buran Ransomware Activity M2

ET TROJAN Buran Ransomware Activity M1

Subscribe to the Proofpoint Blog