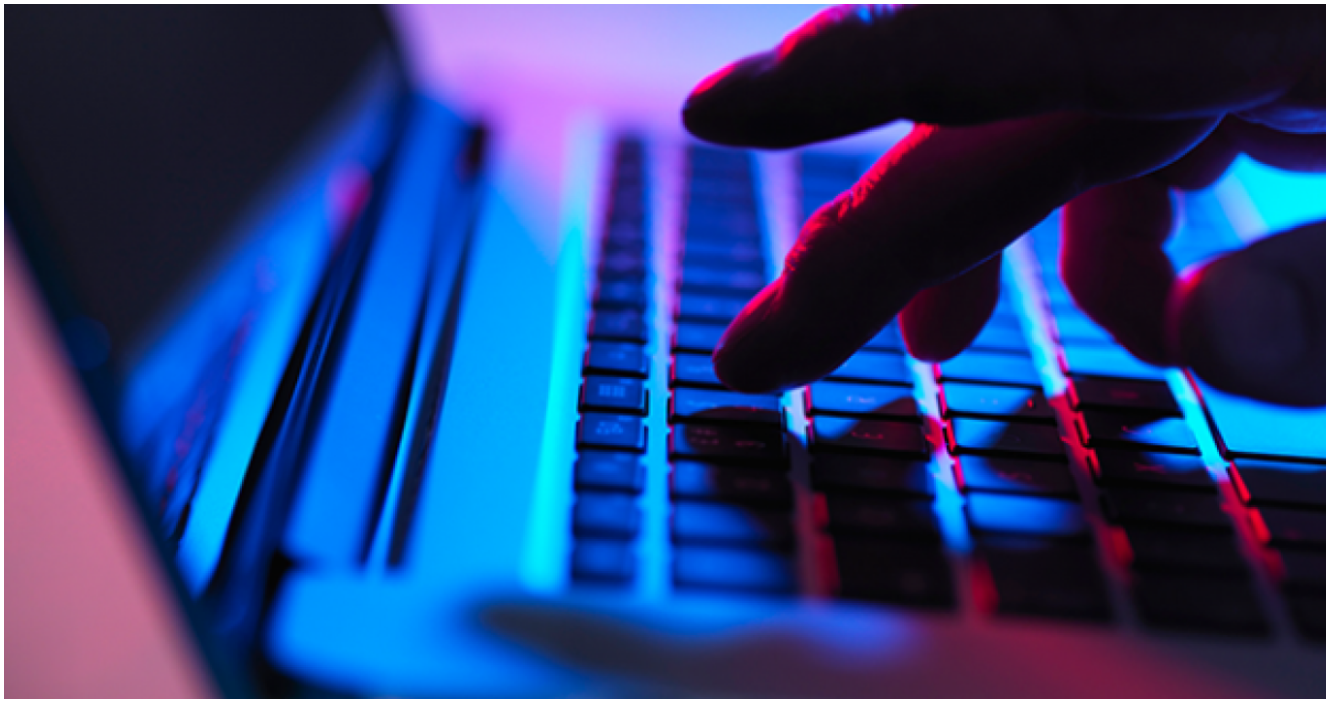
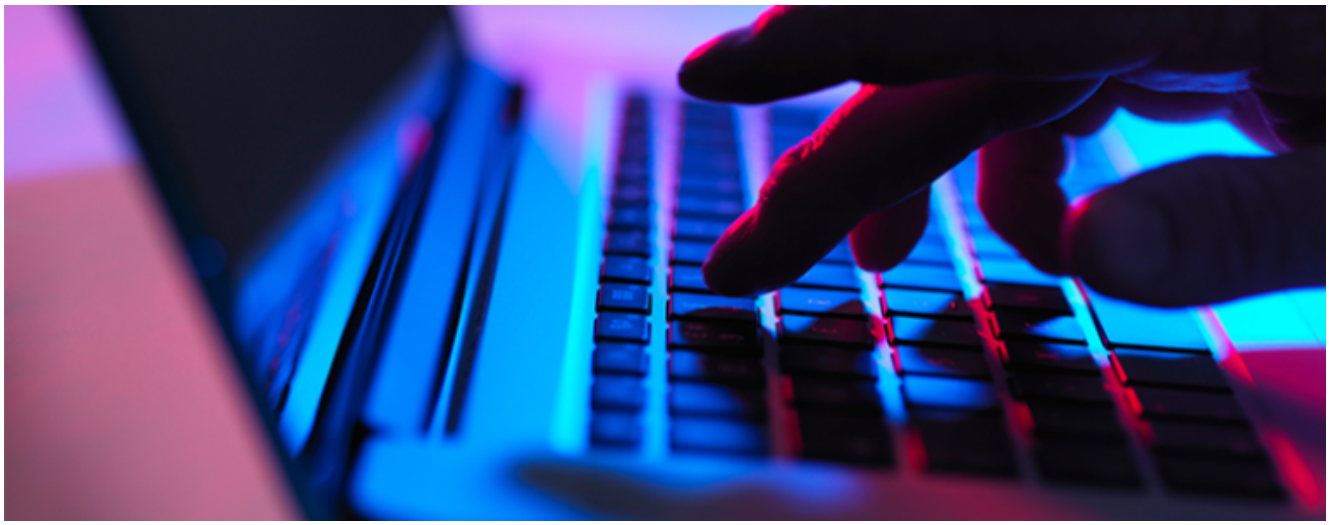
Hakbit Ransomware Campaign Against Germany, Austria, Switzerland

proofpoint.com/us/blog/threat-insight/hakbit-ransomware-campaign-against-germany-austria-switzerland

June 22, 2020



Hakbit Ransomware Campaign Against Germany, Austria, Switzerland



June 22, 2020 Sherrod DeGrippo and the Proofpoint Threat Research Team

Proofpoint researchers have been tracking a low-volume, email-based ransomware campaign targeting organizations in Austria, Switzerland, and Germany. The campaign leverages Hakbit, a variant of Thanos ransomware as a service (RaaS). The attack employs malicious Microsoft Excel attachments delivered from a free email provider (GMX) that primarily serves a European client base. The attachments contain false billing and tax repayment subjects to entice users to enable macros that execute GuLoader, which downloads the ransomware to encrypt files and lock the system.

To help ensure success because Microsoft Office VBA macros do not execute on mobile devices, these emails direct recipients to open attachments on their computer and not their mobile device.

Users targeted were employed in mid-level positions across the pharmaceutical, legal, financial, business service, retail, and healthcare sector. The largest volume of messages we observed were sent to the information technology, manufacturing, insurance, and technology verticals. Proofpoint researchers have observed that the majority of roles targeted in the Hakbit campaigns are customer-facing with individuals' business contact information revealed publicly on company websites, and/or advertisements. These roles include attorneys, client advisors, directors, insurance advisors, managing directors, and project managers.

Below is an example of the lure, many messages arrived with subject lines such as “"Fwd: Steuerrückzahlung" (Translated: Tax Repayment)” and “Ihre Rechnung (Translated: Your Bill)”.

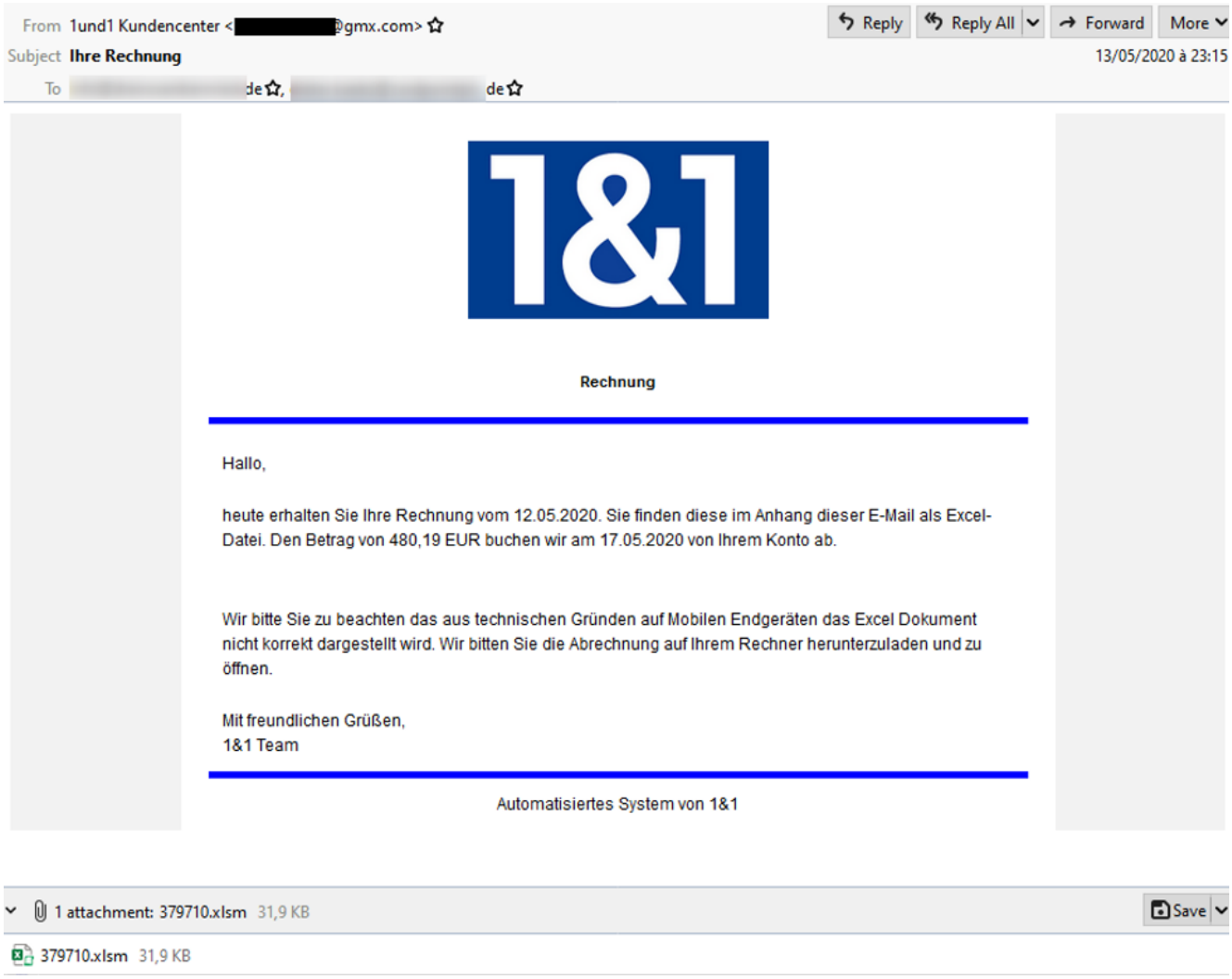


Figure 1 Hakbit Lure Email Message in German

This lure is in German and abuses the logo and branding of 1&1, a German telecommunications company. According to Google Translate, the body of the message states:

> *Today you will receive your invoice dated 12.05.2020. You will find it in the attachment to this e-mail as an Excel file. We will debit the amount of EUR 480.19 from your account on May 17th, 2020.*
>
> *Please note that due to technical reasons the Excel document is not displayed correctly on mobile devices. We ask you to download the invoice on your computer and open it.*
>
> *Best regards,*

The message contains a Microsoft Excel attachment named 379710.xlsm which leverages malicious macros. Because the macros and malware won't work on a mobile device, the message instructs the recipient to use a computer to read the attachment. Once opened, the spreadsheet directs the recipient in German and English to enable macros as shown in Figure 2.

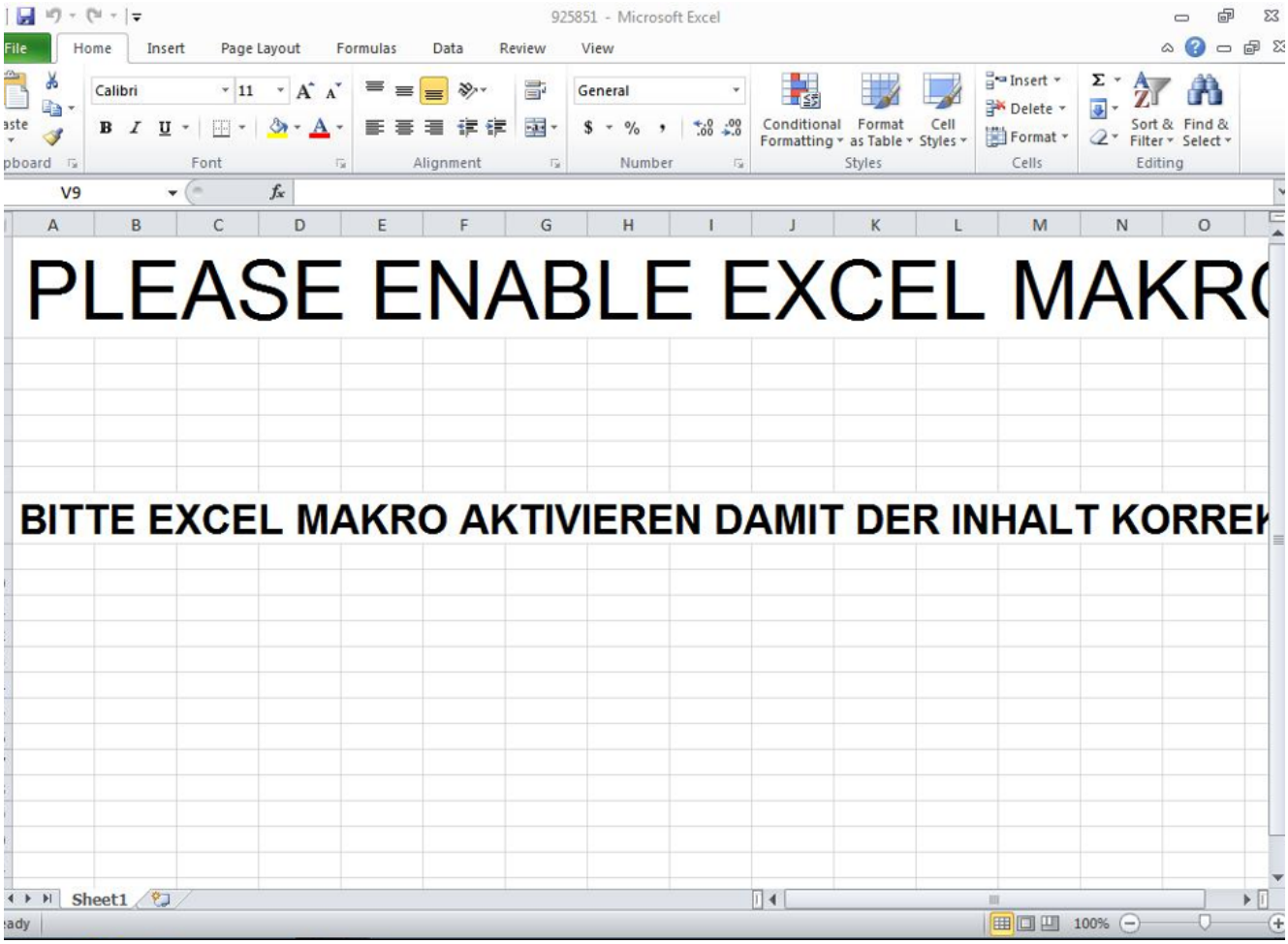
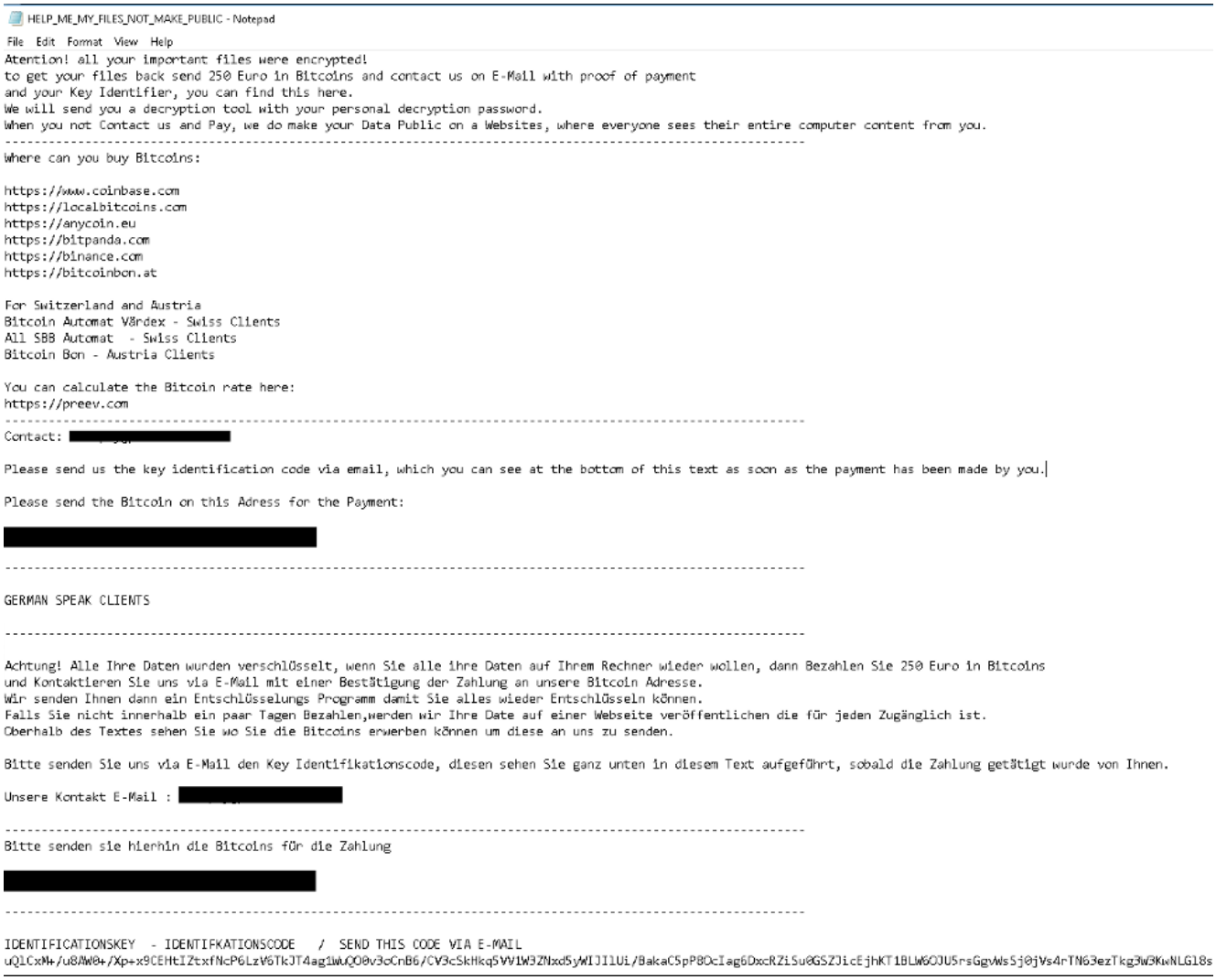


Figure 2 Microsoft Excel Attachment with Enable Macros Message

Once macros are enabled in the spreadsheet, it downloads and executes GuLoader, a relatively new downloader written in VB 6.0 that we wrote about in March 2020. When GuLoader runs, it downloads and executes Hakbit, a ransomware that encrypts files using AES-256 encryption.

Below is the image that appears when Hakbit executes (Figure 3) and the ransom note in both English and German (Figure 4).

Figure 3 Hakbit Ransom Screen



HELP_ME_MY_FILES_NOT_MAKE_PUBLIC - Notepad

File Edit Format View Help

Atention! all your important files were encrypted!
to get your files back send 250 Euro in Bitcoins and contact us on E-Mail with proof of payment
and your Key Identifier, you can find this here.
We will send you a decryption tool with your personal decryption password.
When you not Contact us and Pay, we do make your Data Public on a Websites, where everyone sees their entire computer content from you.

Where can you buy Bitcoins:

https://www.coinbase.com
https://localbitcoins.com
https://anycoin.eu
https://bitpanda.com
https://binance.com
https://bitcoinbon.at

For Switzerland and Austria
Bitcoin Automat Värdex - Swiss Clients
All SBB Automat - Swiss Clients
Bitcoin Bon - Austria Clients

You can calculate the Bitcoin rate here:
https://preev.com

Contact: [redacted]

Please send us the key identification code via email, which you can see at the bottom of this text as soon as the payment has been made by you.

Please send the Bitcoin on this Adress for the Payment:

[redacted]

GERMAN SPEAK CLIENTS

Achtung! Alle Ihre Daten wurden verschlüsselt, wenn Sie alle ihre Daten auf Ihrem Rechner wieder wollen, dann Bezahlen Sie 250 Euro in Bitcoins
und Kontaktieren Sie uns via E-Mail mit einer Bestätigung der Zahlung an unsere Bitcoin Adresse.
Wir senden Ihnen dann ein Entschlüsselungs Programm damit Sie alles wieder Entschlüsseln können.
Falls Sie nicht innerhalb ein paar Tagen Bezahlen,werden wir Ihre Date auf einer Webseite veröffentlichen die für jeden Zugänglich ist.
Oberhalb des Textes sehen Sie wo Sie die Bitcoins erwerben können um diese an uns zu senden.

Bitte senden Sie uns via E-Mail den Key Identifikationscode, diesen sehen Sie ganz unten in diesem Text aufgeführt, sobald die Zahlung getätigt wurde von Ihnen.

Unsere Kontakt E-Mail : [redacted]

Bitte senden sie hierhin die Bitcoins für die Zahlung

[redacted]

IDENTIFICATIONSKEY - IDENTIFKATIONSCODE / SEND THIS CODE VIA E-MAIL
uQlCxN+/u8AW0+/Xp+x9CEHtIZtxfNcP6LzV6TkJT4ag1WuQO0v3oCnB6/CV3cSkHkq5VV1W3ZNxd5yWIJIlUi/BakaC5pP8OcIag6DxcRZiSu0GSZJicEjhKT1BLW6OJU5rsGgvWsSj0jVs4rTN63ezTkg3W3KwNLGl8s

Figure 4 Hakbit Ransom Note

The note demands a payment of 250 Euros in bitcoin to unlock the encrypted files and provides instructions on how to pay the ransom. As of June 16, 2020, our researchers have found no transactions showing payment of the ransom to the bitcoin wallet in the examples here.

Conclusion

Proofpoint researchers have observed consistent low-volume and often boutique ransomware campaigns since January 2020. Proofpoint researchers recently identified a shift in the threat landscape with a large-scale Avaddon ransomware campaign consistent with recent open source vendor reporting. Hakbit exemplifies a people-centric ransomware campaign tailored to a specific audience, role, organization, and in the user's native language.

Indicators of Compromise (IOCs)

Hakbit	**SHA256**	**34b93f1989b272866f023c34a2243978565fcfd23869cacc58ce592c1c545d8e**

Subscribe to the Proofpoint Blog