Ordinypt Ransomware Intentionally Destroys Files, Currently Targeting Germany

bleepingcomputer.com/news/security/ordinypt-ransomware-intentionally-destroys-files-currently-targeting-germany/

Catalin Cimpanu

By
Catalin Cimpanu

- November 9, 2017
- 11:50 AM
- 2

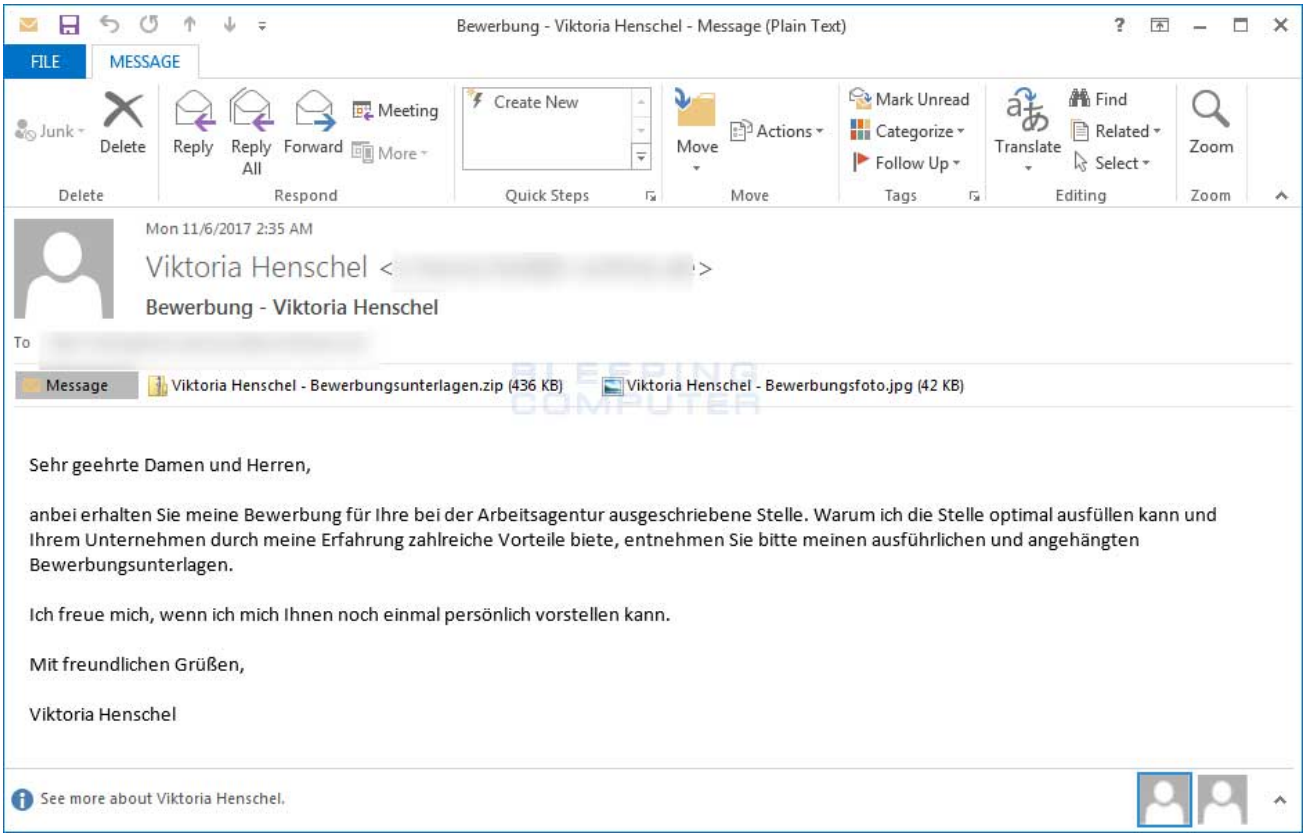
A new ransomware strain called Ordinypt is currently targeting victims in Germany, but instead of encrypting users' documents, the ransomware rewrites files with random data.

This ransomware was first discovered by Michael Gillespie when one of its ransom notes was uploaded to ID-Ransomware. This Monday, G Data security researcher Karsten Hahn, found a sample and discovered that it has been targeting only German users (based on VirusTotal detections) via emails written in German, and delivering ransom notes in an error-free German language.

When originally discovered by Michael, it was named HSDFSDCrypt for lack of a better name, but has since been changed to Ordinypt by G Data.

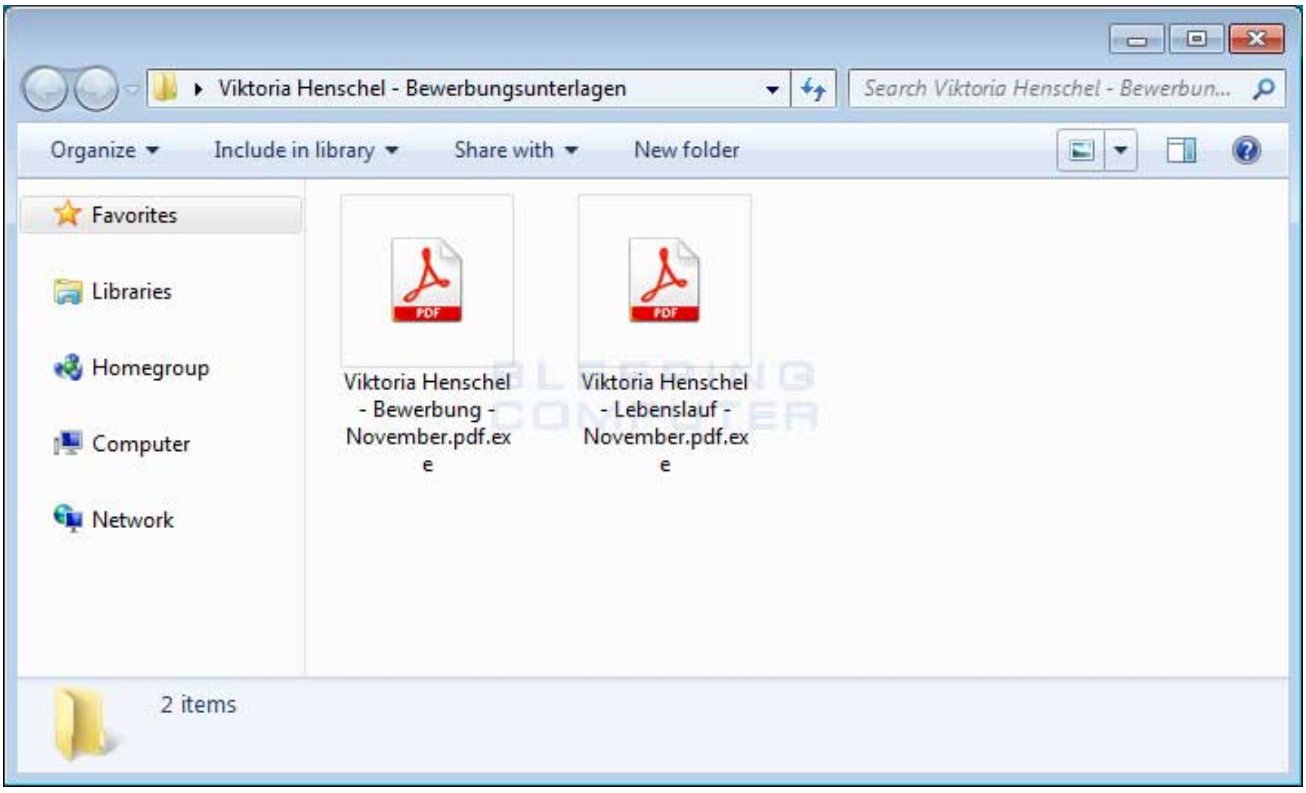
Similar to how the original Petya Ransomware was distributed, Ordinypt is also pretending to be resumes being sent in reply to job adverts. These emails contain two files — a JPG image of the woman supposedly sending a resume, and a ZIP file containing the resume and a curriculum vitae.

These attachments are named **Viktoria Henschel - Bewerbungsfoto.jpg** and **Viktoria Henschel - Bewerbungsunterlagen.zip**.



The ZIP archive contains two EXE files that use the old double-extension and custom icon tricks to fool users into thinking they're different files. In this case, PDF files.

On Windows PCs that hide the file extensions by default, the EXE extension will not show up, and users will only see the PDF part, enough to fool users into believing the files are legitimate PDFs, and not an executables.



Ordinypt replaces files with random data

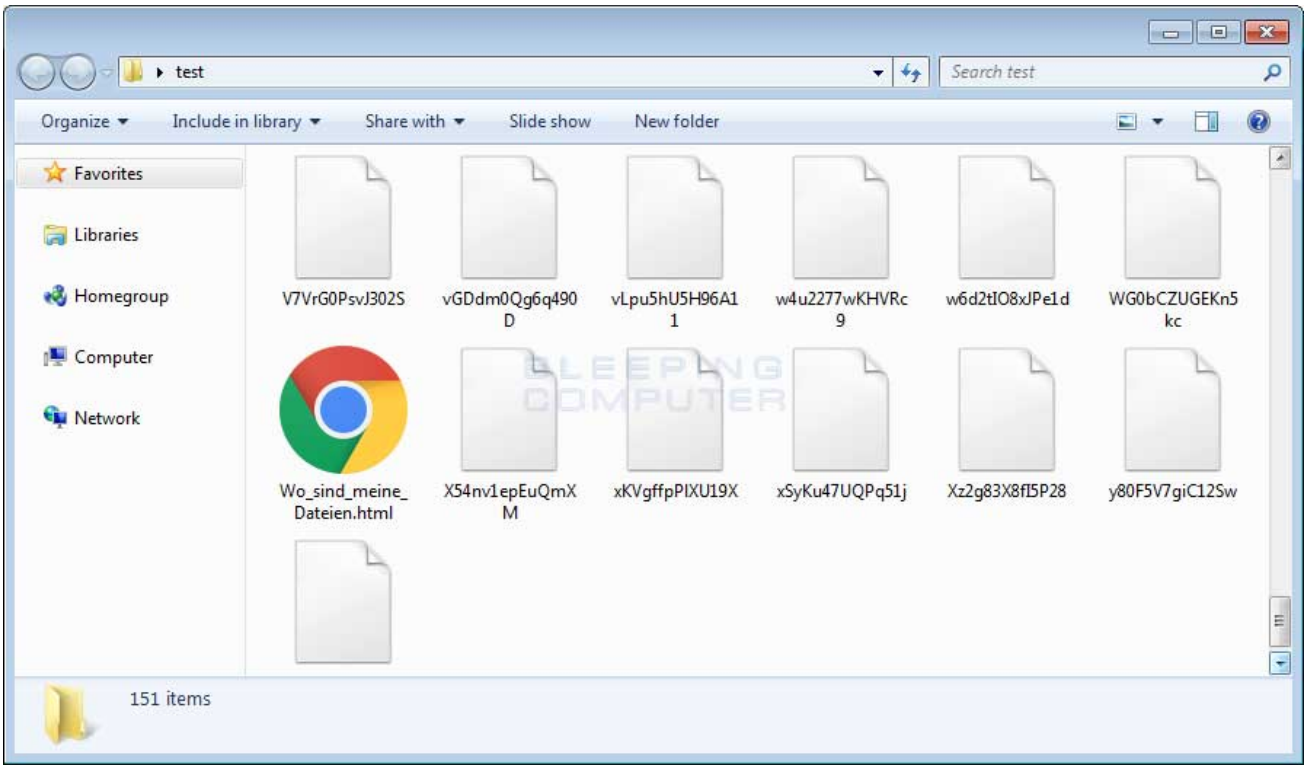
Running either executable will launch the Ordinypt ransomware, or better yet, the Ordinypt wiper. Ordinypt is actually a wiper and not ransomware because it does not bother encrypting anything, but just replaces files with random data.

According to reverse engineer Philipp Mackensen, Ordinypt will replace the contents of files with random generated characters consisting of uppercase and lowercase letters and numbers.

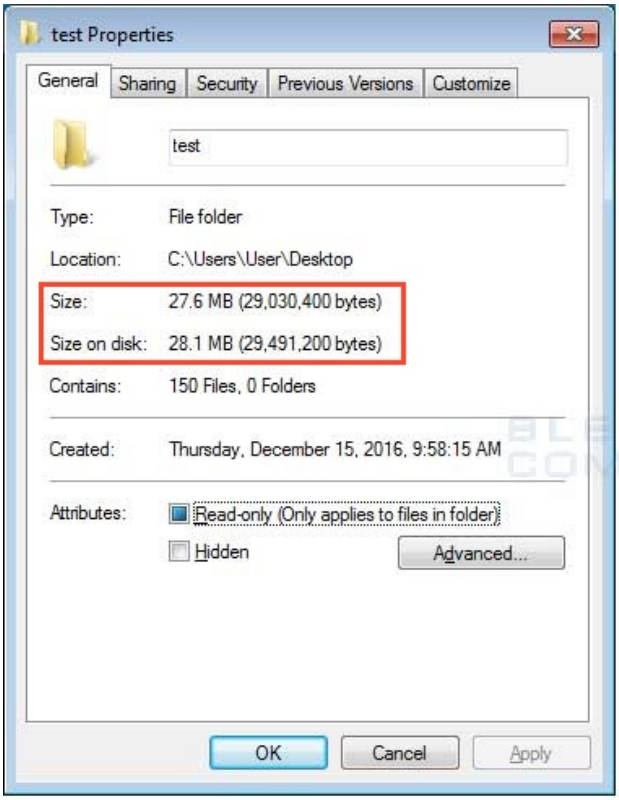
> File names and content are generated by the same function (only needs a length as input) which randomly generates a string that consists of uppercase, lowercase and numeric characters . File size can differ between 8KB and 24KB (also random). Doesn't encrypt .png files tho.
>
> — Philipp Mackensen (@PMackensen) November 9, 2017

Philipp further told *Bleeping Computer* that the wiper performs a search for files just like any other ransomware, but just "creates a "pseudo-encrypted-file" which in reality is just a garbage file and deletes the original file afterwards.". Philipp further went on to say that they were most likely doing this to look like a ransomware, while disguising the fact that it is a wiper.

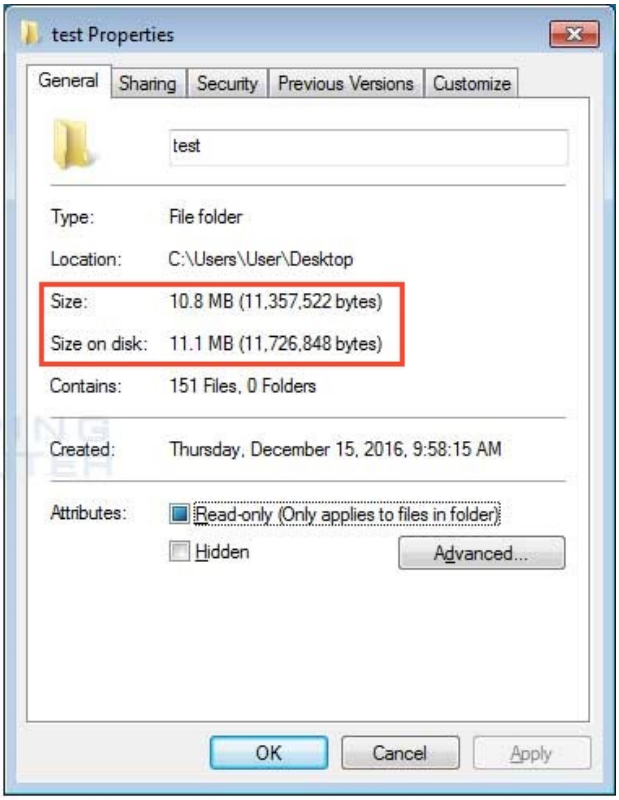
The same algorithm used to generate the random data is also used to generate the new "pseudo-encrypted-file's" name, which is made up of 14 random alpha-numeric characters.



Ordinypt doesn't even bother hiding its destructive nature, as the new files are sometimes more than half the size of the originals.

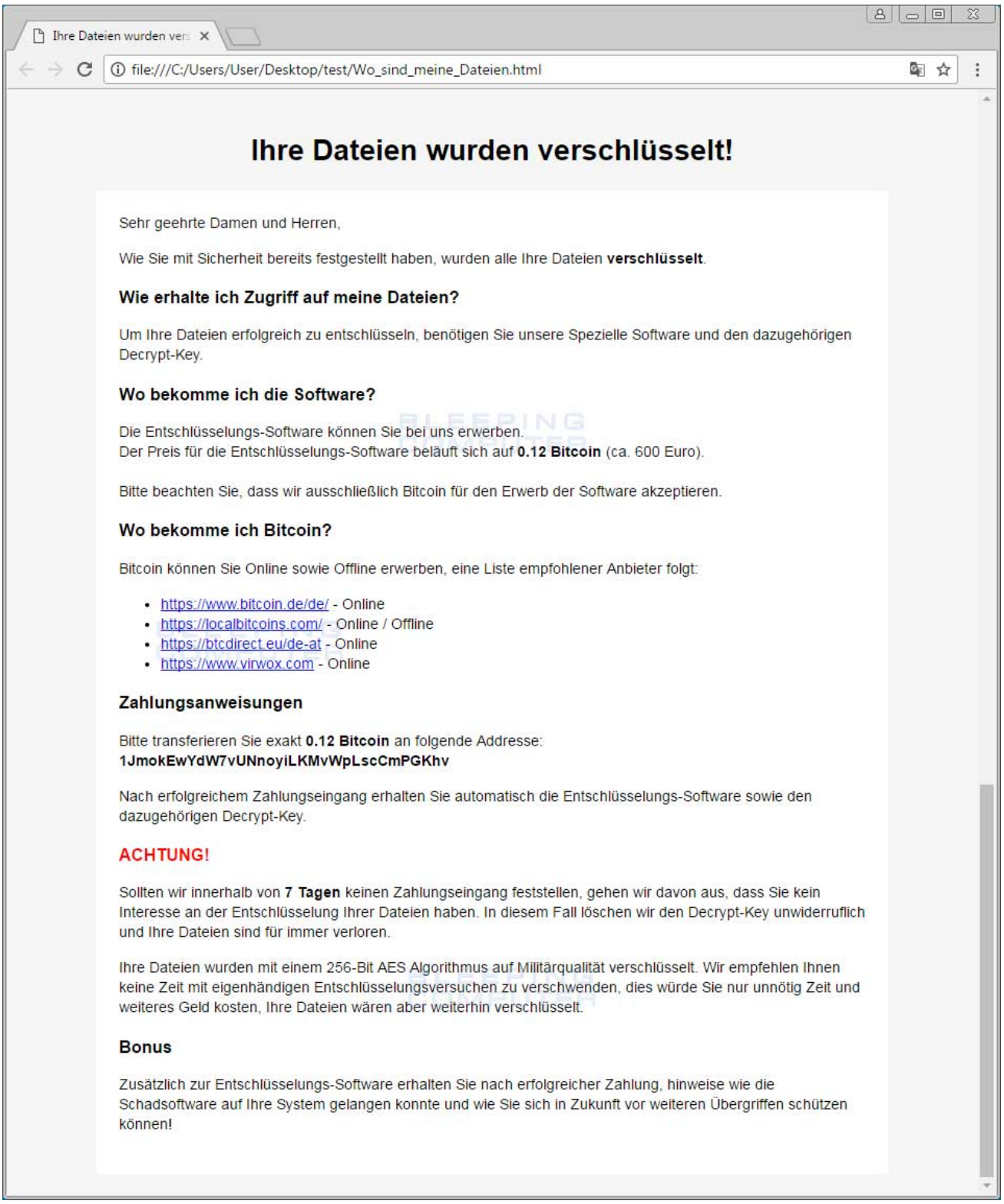


Before Encryption



After Encryption

Ordinypt also drops a ransom note in every folder where it destroys files. The ransom note is named **Wo_sind_meine_Dateien.html**, which translates to Where_are_my_files.html.



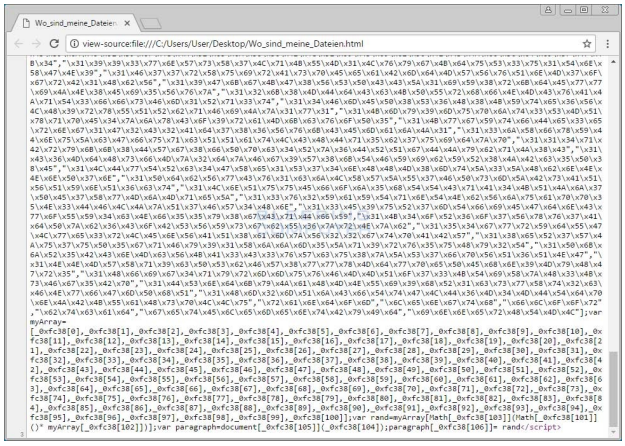
Ordinypt is a wiper disguised as ransomware

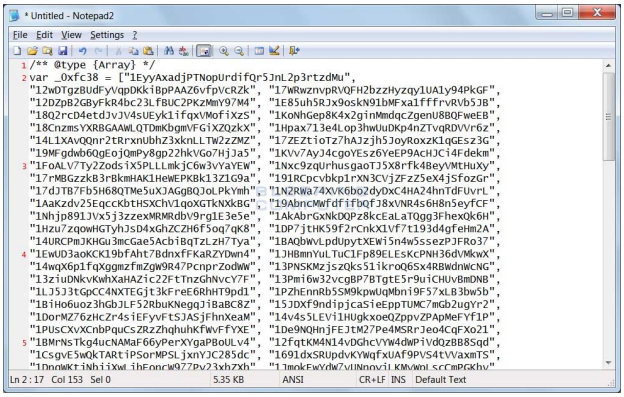
The intentional data destruction behavior is evident in the way the ransom note was coded.

Usually, ransomware strains show an infection ID and a Bitcoin address, Dark Web URL, or email address where victims can contact the ransomware's operator and confirm the ransom payment.

Ordinypt does not list an infection ID, nor does it ask for a file from where the ransomware's authors can extract such an ID.

Instead, Ordinypt's ransom note uses a JavaScript function to select a random Bitcoin address from a list of 101 hardcoded wallet addresses.





Furthermore, there's no way of contacting the faux ransomware's authors and verifying the payment. All evidence points to the fact that someone coded Ordinypt with the intention to damage computers.

The targeting of HR departments via job application emails also speaks volumes about this being an intentional campaign to damage the operations of some Germany-based companies.

Ordinypt is not the first wiper disguised as ransomware. The most famous case is NotPetya, the faux ransomware that hit the Ukraine in late June, but quickly spread to companies all over the world.

IOCs:

Ordinypt / HSDFSDCrypt Hash:

SHA256: 085256b114079911b64f5826165f85a28a2a4ddc2ce0d935fa8545651ce5ab09

Ordinypt / HSDFSDCrypt Spam email text:

Sehr geehrte Damen und Herren,

anbei erhalten Sie meine Bewerbung für Ihre bei der Arbeitsagentur ausgeschriebene Stelle. Warum ich die Stelle optimal ausfüllen kann und Ihrem Unternehmen durch meine Erfahrung zahlreiche Vorteile biete, entnehmen Sie bitte meinen ausführlichen und angehängten Bewerbungsunterlagen.

Ich freue mich, wenn ich mich Ihnen noch einmal persönlich vorstellen kann.

Mit freundlichen Grüßen,

Viktoria Henschel

Translated Spam:

Dear Sir or Madam,

Enclosed you will receive my application for your job advertised at the Employment Agency. Please see my detailed and attached application documents for the reasons why I am able to fill the vacant position optimally and that your experience has many advantages for your company.

I'm glad if I can introduce myself once again.

Best regards,

Viktoria Henschel

Ordinypt / HSDFSDCrypt Ransom note text:

Ihre Dateien wurden verschlüsselt!

Sehr geehrte Damen und Herren,

Wie Sie mit Sicherheit bereits festgestellt haben, wurden alle Ihre Dateien verschlüsselt.

Wie erhalte ich Zugriff auf meine Dateien?

Um Ihre Dateien erfolgreich zu entschlüsseln, benötigen Sie unsere Spezielle Software und den dazugehörigen Decrypt-Key.

Wo bekomme ich die Software?

Die Entschlüsselungs-Software können Sie bei uns erwerben.
Der Preis für die Entschlüsselungs-Software beläuft sich auf 0.12 Bitcoin (ca. 600 Euro).

Bitte beachten Sie, dass wir ausschließlich Bitcoin für den Erwerb der Software akzeptieren.

Wo bekomme ich Bitcoin?

Bitcoin können Sie Online sowie Offline erwerben, eine Liste empfohlener Anbieter folgt:

https://www.bitcoin.de/de/ - Online
https://localbitcoins.com/ - Online / Offline
https://btcdirect.eu/de-at - Online
https://www.virwox.com - Online
Zahlungsanweisungen

Bitte transferieren Sie exakt 0.12 Bitcoin an folgende Addresse:
14DeorRVAaqEeLugPHhcHdejyEAL26gdpx

Nach erfolgreichem Zahlungseingang erhalten Sie automatisch die Entschlüsselungs-Software sowie den dazugehörigen Decrypt-Key.

ACHTUNG!

Sollten wir innerhalb von 7 Tagen keinen Zahlungseingang feststellen, gehen wir davon aus, dass Sie kein Interesse an der Entschlüsselung Ihrer Dateien haben. In diesem Fall löschen wir den Decrypt-Key unwiderruflich und Ihre Dateien sind für immer verloren.

Ihre Dateien wurden mit einem 256-Bit AES Algorithmus auf Militärqualität verschlüsselt. Wir empfehlen Ihnen keine Zeit mit eigenhändigen Entschlüsselungsversuchen zu verschwenden, dies würde Sie nur unnötig Zeit und weiteres Geld kosten, Ihre Dateien wären aber weiterhin verschlüsselt.

Bonus

Zusätzlich zur Entschlüsselungs-Software erhalten Sie nach erfolgreicher Zahlung, hinweise wie die Schadsoftware auf Ihre System gelangen konnte und wie Sie sich in Zukunft vor weiteren Übergriffen schützen können!

Related Articles:

Beware: Onyx ransomware destroys files instead of encrypting them

BlackCat/ALPHV ransomware asks $5 million to unlock Austrian state

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

- Germany
- HSDFSDCrypt
- Ordinypt
- Ransomware
- Wiper

Catalin Cimpanu

Catalin Cimpanu is the Security News Editor for Bleeping Computer, where he covers topics such as malware, breaches, vulnerabilities, exploits, hacking news, the Dark Web, and a few more. Catalin previously covered Web & Security news for Softpedia between May 2015 and October 2016. The easiest way to reach Catalin is via his XMPP/Jabber address at campuscodi@xmpp.is. For other contact methods, please visit Catalin's author page.

- Previous Article
- Next Article

Comments

- 
  RJMass1 - 4 years ago
  -
  -
  Great article!!

- 

  worstanalyst - 4 years ago

  -
  -

  This article is very informative - so thank you very much for that. You mentioned, that there are 101 BTC-addresses hardcoded. Has anyone a list of them in txt-format? Would be a very good starting point for a Bitcoin-Tracing - probably some people will be willing to pay...

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: