

[Blog Home \(https://blog.checkpoint.com/\)](https://blog.checkpoint.com/) > [Research \(https://blog.checkpoint.com/research/\)](https://blog.checkpoint.com/research/) >

Looking for a New Employee? Beware of a New Ransomware Campaign

Filter by:

Select category

Search Articles



[\(HTTPS://BLOG.CHECKPOINT.COM
/RESEARCH/\)](https://blog.checkpoint.com/research/)

JANUARY 3, 2017


Looking for a New Employee? Beware of a New Ransomware Campaign




By **Check Point Research Team**




SHARE Despite trying to brand itself as a new malware, GoldenEye, the latest Petya variant, is very similar to older versions and differs mostly in its “golden” motif. The most prominent change, however, is how the


 campaign spreads the ransomware (<https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-ransomware/>) (<https://www.facebook.com/sharer.php?u=https%3A%2F%2Fblog.checkpoint.com%2Fresearch%2Flooking-new-employee-beware-new-ransomware-campaign%2F>)

 The current campaign used to distribute GoldenEye has a job application theme. It is therefore aimed at companies’ Human Resources departments, due to the fact they usually cannot avoid opening emails and

<https://twitter.com/shane2ent/status/1518751436012416000> attachments <https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-ransomware/> as a common malware infection method. ([text=Looking%20for%20a%20New%20Employee%20Beware%20of%20a%20New%20Ransomware%20Campaign](https://twitter.com/shane2ent/status/1518751436012416000?text=Looking%20for%20a%20New%20Employee%20Beware%20of%20a%20New%20Ransomware%20Campaign))

HR-Targeted Ransomware

 The new campaign targets German speakers and mimics a job application. The email contains a brief message supposedly from a job applicant and contains two attachments as can be seen below. (<https://www.linkedin.com/shareArticle?mini=true&url=https%3A%2F%2Fblog.checkpoint.com%2Fresearch%2Flooking-new-employee-beware-new-ransomware-campaign%2F>)

 The first attachment is a PDF containing a cover letter which has no malicious content and its primary purpose is to lull the victim into a false sense of security. The second attachment is an Excel file with malicious macros unbeknown to the receiver. It contains a picture of a flower with the word “Loading...” underneath, and a text in German asking the victim to enable content so that the macros can run. (<https://www.reddit.com/submit?url=https%3A%2F%2Fblog.checkpoint.com%2Fresearch%2Flooking-new-employee-beware-new-ransomware-campaign%2F>)


 (<mailto:?subject=Looking%20for%20a%20New%20Employee%20Beware%20of%20a%20New%20Ransomware%20Campaign&body=https%3A%2F%2Fblog.checkpoint.com%2Fresearch%2Flooking-new-employee-beware-new-ransomware-campaign%2F>)

Image 1: Screenshot of the email campaign

petya-1 (<http://blog.checkpoint.com/wp-content/uploads/2017/01/petya-1.jpg>)

Image 2: The PDF Cover letter, with no malicious content

petya-2 (<http://blog.checkpoint.com/wp-content/uploads/2017/01/petya-2.jpg>)

Check Point security researchers observed the spam campaign running in the past few days, and identified that Excel files have different names. They follow a similar concept, starting with a name of a job-seeking “candidate”, and the word “application” in German (“*Bewerbung*”):

Wiebold-Bewerbung.xls

Meinel-Bewerbung.xls

Seidel-Bewerbung.xls

Wüst-Bewerbung.xls

Born-Bewerbung.xls

Schlosser-Bewerbung.xls

Image 3: The Excel file requesting to run macros

petya-3 (<http://blog.checkpoint.com/wp-content/uploads/2017/01/petya-3.jpg>)

Encryption Process

When a user clicks “Enable Content”, the code inside the macro executes and initiates the process of encrypting the files, denying the victim access to his or her files.

GoldenEye then, appends a random 8-character extension to each encrypted file. After all the files are encrypted, GoldenEye presents the ransom note: “YOUR_FILES_ARE_ENCRYPTED.TXT”

After displaying the ransom note, GoldenEye forces a reboot and starts encrypting the disk. This action makes it impossible to access any files on the hard disk. While the disk undergoes encryption, the victim sees a fake “chkdsk” screen, as in previous Petya variants.

Image 4: fake “chkdsk” screen

petya-4 (<http://blog.checkpoint.com/wp-content/uploads/2017/01/petya-4.jpg>)

Following the encryption of the disk, the victim is presented with a boot-level ransom note.

petya-4-5 (<http://blog.checkpoint.com/wp-content/uploads/2017/01/petya-4.5.jpg>)

The ransom note content is the same as in previous Petya variants; however, GoldenEye uses a yellow colored text instead of red or green.

petya-5 (<http://blog.checkpoint.com/wp-content/uploads/2017/01/petya-5.jpg>)

The victim is presented with a “personal decryption code”, which he can enter in a Dark Web portal in order to pay the ransom. The Dark Web portal includes a support page, where victims can send messages to the GoldenEye admin if they have issues with the payment or decryption process.

The current ransom demanded by GoldenEye begins at 1.3 BitCoins (BTC), which are approximately \$1,000, with observed figures between 1.33 and 1.39 BTC. We can assume that the actor behind GoldenEye aims to receive \$1,000 for each infection, and so the actual ransom amount varies according to BTC price fluctuation.

The developer behind Petya is a cyber-criminal who goes by the name of Janus. Up to October 2016, Janus ran the “Janus Cybercrime” website, where Petya was offered in combination with another ransomware, Mischa, as a *Ransomware-as-a-Service*. Janus is also the name of the cybercrime syndicate that was

featured in the James Bond film *GoldenEye*, released in 1995.

A Non-Coincidental Resemblance

If the Bewerbung campaign sounds familiar, it is probably because it was used in the past by the Cerber ransomware [3]. As both Petya/GoldenEye and Cerber act as ransomware as-a-service (RaaS), it is very likely that there is one threat actor leveraging the German CV campaign to send both malware types to his/her victims.

How Can You Stay Protected?

Check Point SandBlast Zero Day Protection (<https://www.checkpoint.com/products-solutions/zero-day-protection/>) Blade protects against this threat.

A Check Point Forensics report of this threat can be seen here (<http://freports.us.checkpoint.com/petya-ge/>).

References:

1. "Petya – Taking Ransomware to the Low Level." Blog post. Malwarebytes Labs. Malwarebytes, 01 Apr. 2016. Web. 07 Dec. 2016. <<https://blog.malwarebytes.com/threat-analysis/2016/04/petya-ransomware> (<https://blog.malwarebytes.com/threat-analysis/2016/04/petya-ransomware>)/>.
2. Cimpanu, Catalin. "Petya Ransomware Returns with GoldenEye Version, Continuing James Bond Theme." Blog post. BleepingComputer. Bleeping Computer® LLC, 06 Dec. 2016. Web. 07 Dec. 2016. <<https://www.bleepingcomputer.com/news/security/petya-ransomware-returns-with-goldeneye-version-continuing-james-bond-theme> (<https://www.bleepingcomputer.com/news/security/petya-ransomware-returns-with-goldeneye-version-continuing-james-bond-theme>)/>.
3. Check Point Threat Intelligence Research Team. "CerberRing: An In-Depth Exposé on Cerber Ransomware-as-a-Service." Blog post. Check Point Blog. Check Point Software Technologies Ltd., 16 Aug. 2016. Web. 14 Dec. 2016. <<http://blog.checkpoint.com/2016/08/16/cerberring> (<http://blog.checkpoint.com/2016/08/16/cerberring>)/>.

○ You may also like





(<https://blog.checkpoint.com/artificial-intelligence/breaking-gpt-4-bad-check-point-research-exposes-how-security-boundaries-can-be-breached-as-machines-wrestle-with-inner-conflicts/>)
JUNE 26, 2023

Breaking GPT-4 Bad: Check Point Research Exposes How Security Boundaries Can Be Breached as Machines Wrestle with Inner...

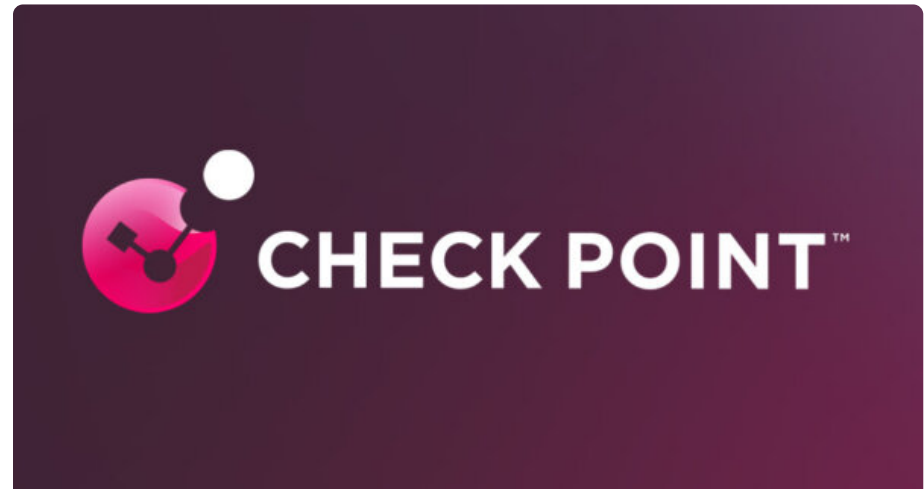
Highlights Check Point Research examines security and safety aspects of ...



(<https://blog.checkpoint.com/security/latest-chinese-state-sponsored-attacks-on-critical-us-infrastructure-spies-a-continuation-of-trend-reports-check-point-research/>)
MAY 25, 2023

Latest Chinese state-sponsored attacks on critical US infrastructure spies a continuation of trend, Reports Check Point Research...

Last Wednesday, Microsoft issued a warning claiming Chinese state-sponsored hackers ...



(<https://blog.checkpoint.com/security/check-point-research-reveals-a-malicious-firmware-implant-for-tp-link-routers-linked-to-chinese-apt-group/>)
 (HTTPS://BLOG.CHECKPOINT.COM/RESEARCH/) MAY 16, 2023

Check Point Research reveals a malicious firmware implant for TP-Link routers, linked to Chinese APT group...

Highlights Check Point Research (CPR) exposes a malicious firmware implant ...

(<https://blog.checkpoint.com/security/april-2023s-most-wanted-malware-qbot-launches-substantial-malspam-campaign-and-mirai-makes-its-return/>)
 (HTTPS://BLOG.CHECKPOINT.COM/RESEARCH/) MAY 11, 2023

April 2023's Most Wanted Malware: Qbot Launches Substantial Malspam Campaign and Mirai Makes its Return...

Check Point Research uncovered a substantial malspam campaign for Trojan ...

Follow Us  (<https://www.facebook.com/checkpointsoftware>) 
 (<https://twitter.com/checkpointsw>)  (<https://www.linkedin.com/company/check-point-software-technologies>)  (<https://www.youtube.com/user/CPGlobal>)

YOU DESERVE THE BEST SECURITY™

©1994-2023 Check Point Software Technologies Ltd. All rights reserved.

Copyright (<https://www.checkpoint.com/copyright/>) | Privacy Policy (<https://www.checkpoint.com/privacy/>)