Lampion Trojan Utilizes New Delivery through Cloud-Based Sharing

cofense.com/blog/lampion-trojan-utilizes-new-delivery-through-cloud-based-sharing

Cofense September 9, 2022

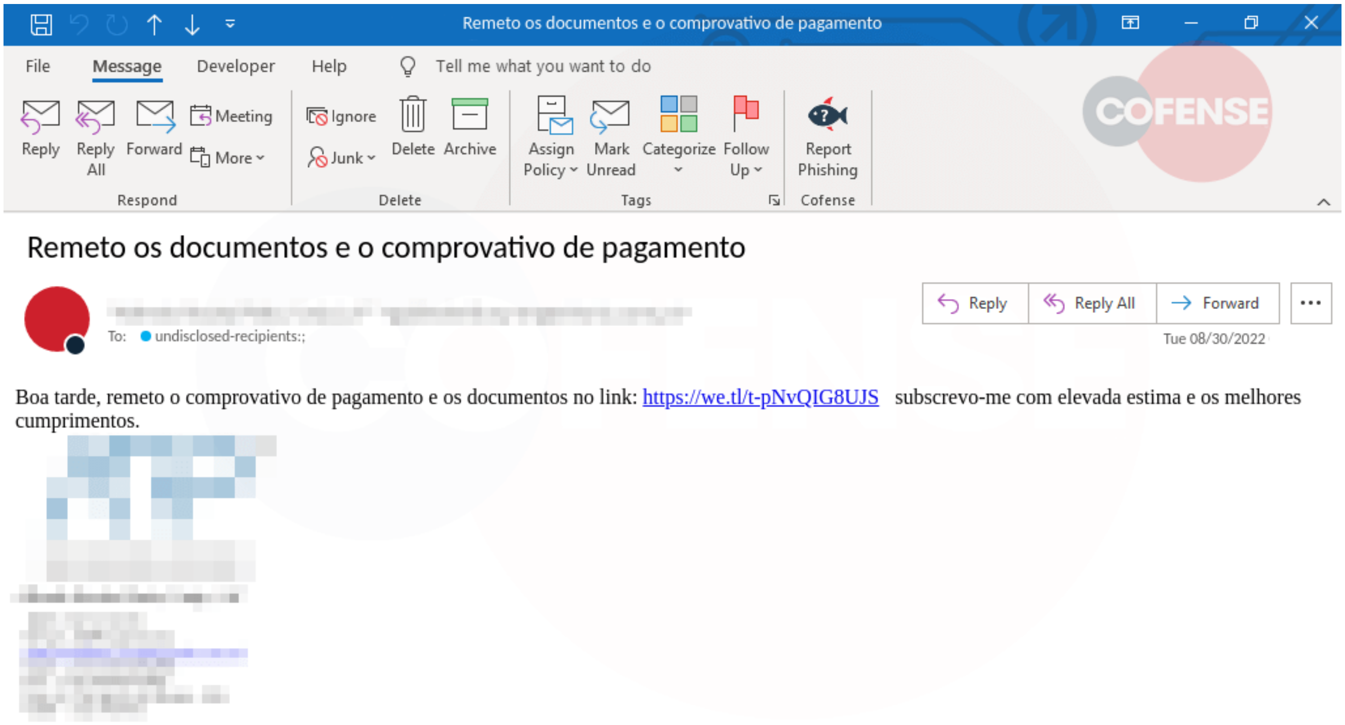
Found in Environments Protected By:

Microsoft

By Andy Mann and Dylan Main, Cofense Phishing Defense Center

Analysts at the Cofense Phishing Defense Center (PDC) have recently analyzed an email asking users to download a “Proof of Payment” as well as other documents. While it is important to never click on the link(s) or download the attachment(s) of any suspicious email, if the recipient interacts with the link, it downloaded the malware Lampion.

The Lampion banking trojan has been around since 2019, but this is the first time it has been analyzed by the PDC. While it has not yet been determined who exactly is behind the malware, it is known for using a VBS loader. Fortunately, threat actors have been spotted by PDC analyst using a new form of delivery for that very VBS file. Using the trusted cloud platform used for payments, WeTransfer, threat actors are attempting to gain the trust of users while taking advantage of the service provided by the popular site. By leveraging a trusted payment site, it’s not surprising to see threat actors align their email message for this process. A well-conditioned user quickly reported this email that mitigated the threat of the malware infection.



Remeto os documentos e o comprovativo de pagamento

[redacted]

To: undisclosed-recipients:;

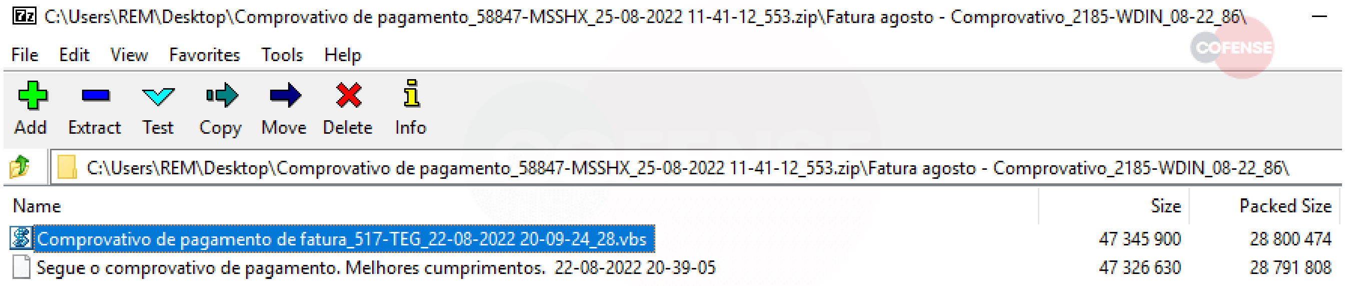
Tue 08/30/2022

Boa tarde, remeto o comprovativo de pagamento e os documentos no link: https://we.tl/t-pNvQIG8UJS subscrevo-me com elevada estima e os melhores cumprimentos.

[redacted]

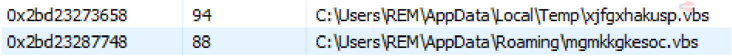
Figure 1: Email Body
English translation: Good afternoon, I send proof of payment and documents on the link: hXXps://we[.]tl/t-pNvQIG8UJS I subscribe with high esteem and best regards

In Figure 1, the threat actor used a very simple email message to engage the recipient. The strongest tactic taken would is spoofing a legitimate company, which could potentially be a result of compromised credentials. The email sent to the recipient is sent a proof of payment and other documents, which are accessible at the URL hXXps://we[.]tl/t-pNvQIG8UJS. When the recipient interacts with the URL they are directed to the page where they can download a ZIP file containing the documents referenced in the email.



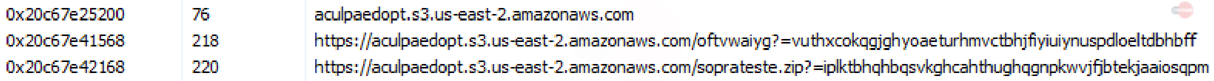
```
C:\Users\REM\Desktop\Comprovativo de pagamento_58847-MSSHX_25-08-2022 11-41-12_553.zip\Fatura agosto - Comprovativo_2185-WDIN_08-22_86\

Name                                                                                  Size   Packed Size
Comprovativo de pagamento de fatura_517-TEG_22-08-2022 20-09-24_28.vbs          47 345 900    28 800 474
Segue o comprovativo de pagamento. Melhores cumprimentos.  22-08-2022 20-39-05  47 326 630    28 791 808
```

Figure 2: Contents of the ZIP File



```
0x2bd23273658    94    C:\Users\REM\AppData\Local\Temp\xjfgxhakusp.vbs
0x2bd23287748    88    C:\Users\REM\AppData\Roaming\mgmkkgkesoc.vbs
```

Figure 3: Strings from the First Wscript Process Once the ZIP file is downloaded, its contents can be extracted to reveal a folder containing the two files seen in Figure 2. The VBS file, Comprovativo de pagamento de fatura_517-TEG_22-08-2022 20-09-24_28.vbs, is the file of concern as this launches the script, to lead the malicious process. Next, it will initiate a wscript process. Analyzing the strings in the memory of this process will result in finding references to two different VBS files, seen in Figure 3. This initial process created these files in the AppData\Local\Temp and AppData\Roaming directories. There are four VBS files created in total, each with random letters as a filename. The scripts in AppData\Roaming are less relevant. One file appears to be empty or was deleted during the process while the other is small with minimal functionality. The script, xjfgxhakusp.vbs, in AppData\Local\Temp is far more important.



```
0x20c67e25200    76     aculpaedopt.s3.us-east-2.amazonaws.com
0x20c67e41568    218    https://aculpaedopt.s3.us-east-2.amazonaws.com/oftvwaiyg?=vuthxcokqgjghyoaeturhmvctbhjfiyiuiynuspdloeltdbhbff
0x20c67e42168    220    https://aculpaedopt.s3.us-east-2.amazonaws.com/soprateste.zip?=iplktbhqhbqsvkghcahthughqgnpkwvjfjbtekjaaiosqpm
```

Figure 4: URLs Leading to DLLs While there are two VBS files in AppData\Local\Temp, the smaller script is only meant to initiate the other, larger script, xjfgxhakusp.vbs. It is a strange extra step taken by the threat actor. Upon running the larger script, another wscript process is initiated. This second wscript process reaches out to the two payload URLs in Figure 4. Both download the final DLL files. The bottom URL will download a password protected ZIP which holds the DLL, but the password is hardcoded into the malicious process itself. The DLLs are then finally injected into the memory. As a banking Trojan, the Lampion mainly looks to steal the targets valuable information.

While email security continues to evolve to protect the organization, threat actors are constantly looking for opportunities to land in the inbox. This is why it is critical to provide your users with simulations aligned with the latest threats. Customers of the Cofense PDC can ease or confirm their suspicions by reporting suspicious emails to the PDC where an analyst will analyze the email for emerging threats. Contact us to learn more.

Indicators of Compromise	IP
hXXps://we[.]tl/t-pNvQIG8UJS	13[.]249[.]39[.]48
hXXps://wetransfer[.]com/downloads/d8c6430f0c15ee79cb72ea2083f4a07420220830135534/b872b1	108[.]128[.]47[.]24
hXXps://aculpaedopt[.]s3[.]us-east-2[.]amazonaws[.]com/soprateste.zip?=ttvuawzgbpiqawlaarfnlxatyebabbwpriceiqupxmmzuix	52[.]219[.]104[.]24
hXXps://aculpaedopt[.]s3[.]us-east-2[.]amazonaws[.]com/oftvwaiyg?=wiyjxpnveuzmgakjpgcjitnjwxaizzzbzmibklzkokxitcgpmso	52[.]219[.]177[.]178

All third-party trademarks referenced by Cofense whether in logo form, name form or product form, or otherwise, remain the property of their respective holders, and use of these trademarks in no way indicates any relationship between Cofense and the holders of the trademarks. Any observations contained in this blog regarding circumvention of end point protections are based on observations at a point in time based on a specific set of system configurations. Subsequent updates or different configurations may be effective at stopping these or similar threats. Past performance is not indicative of future results.