Related Insights

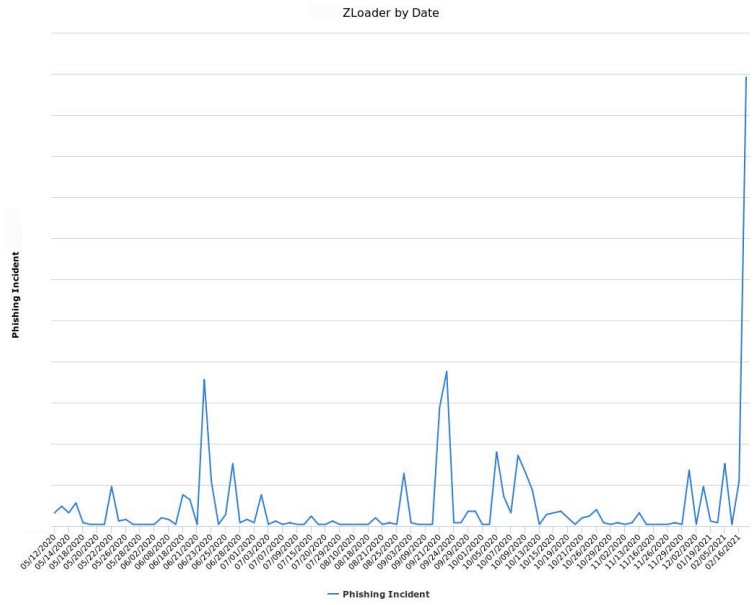
info.phishlabs.com/blog/surge-in-zloader-attacks-observed

February 23, 2021

Get The Latest Insights

By Jessica Ellis | February 23, 2021

PhishLabs has observed a spike in malicious emails distributing ZLoader malware. The spike is notably one of the greatest upticks for a single payload observed in a 24-hour period over the past year, and is the first significant sign that another botnet may be stepping up in the aftermath of the Emotet takedown.



May 2020 – February 2021 ZLoader Activity

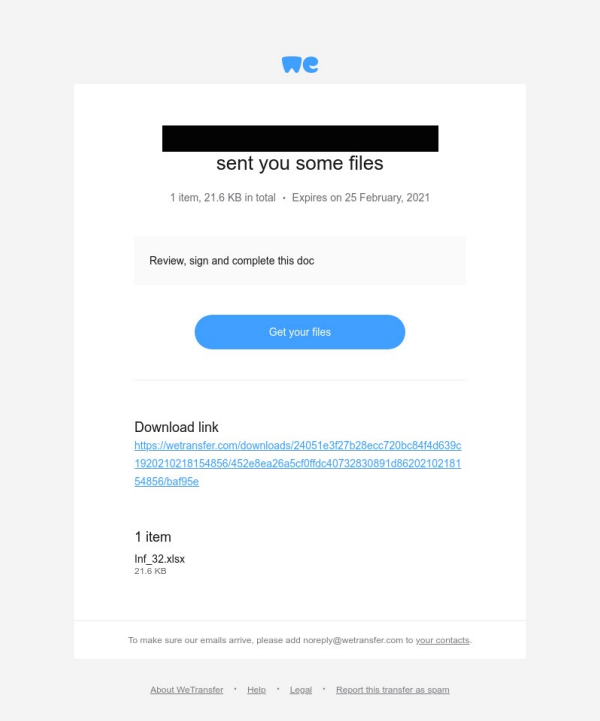
ZLoader is one of the most frequently reported malware strains since June 2020. This particular campaign uses three legitimate file sharing platforms to distribute attacks: WeTransfer, Google Docs, and box.com. Emails are delivered through a variety of compromised accounts. The payload is delivered via malicious files and download links.

WeTransfer Example

WeTransfer Sender Address: **
WeTransfer Subject Line: *sent you files via WeTransfer*

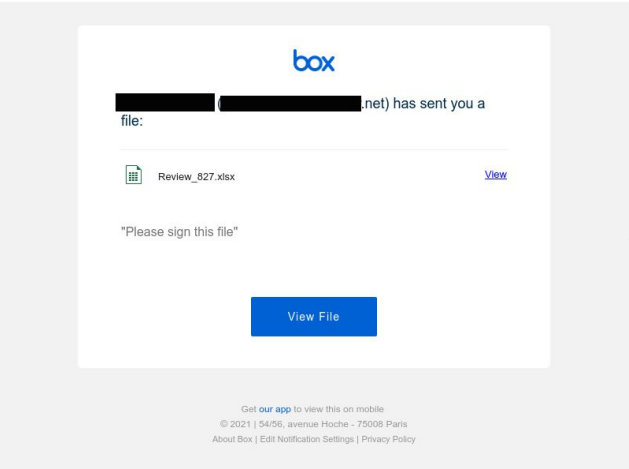
WeTransfer URL:

hxxps://wetransfer[.]com/downloads/52d55eeb42591d9ebbffe5326326858320210218183005/8b80cbbd9c1b8f7695b8de69e995ebee20210218183
utm_campaign=WT_email_tracking&utm_content=general&utm_medium=download_button&utm_source=notify_recipient_email

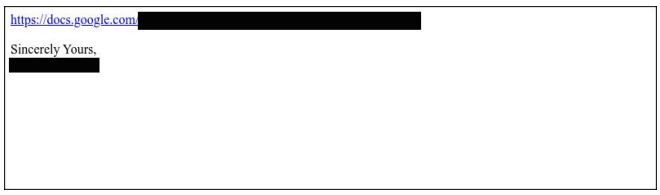


WeTransfer Phishing Lure

Additional Lures



Box.com Phishing Lure



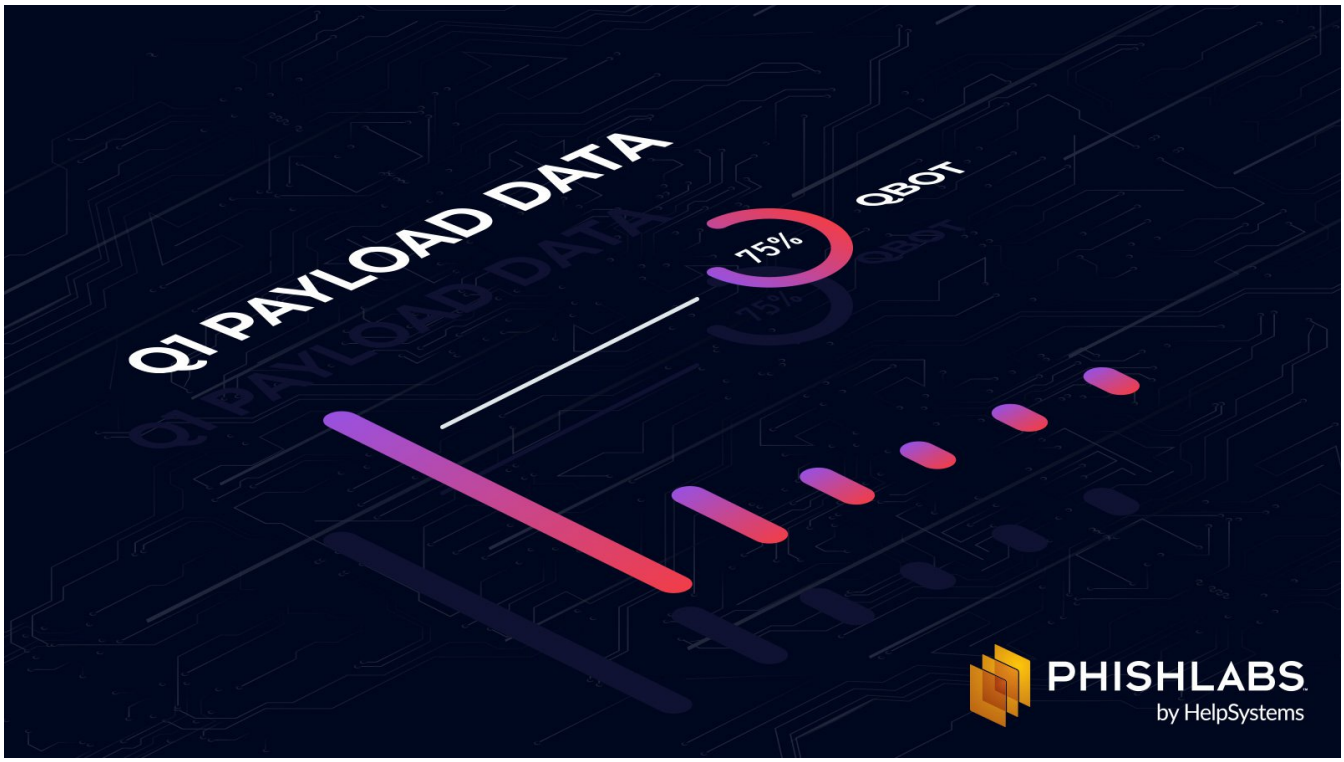
Google Docs Phishing Lure

ZLoader is a popular banking trojan often purchased for distribution by threat actors through Malware-as-a-Service (MaaS). It is a derivative of the Zeus banking trojan and commonly known for stealing victim's credentials through web injects.

ZLoader is delivered through email phishing and there are indications that it is linked to Ryuk and Egregor ransomware strains.

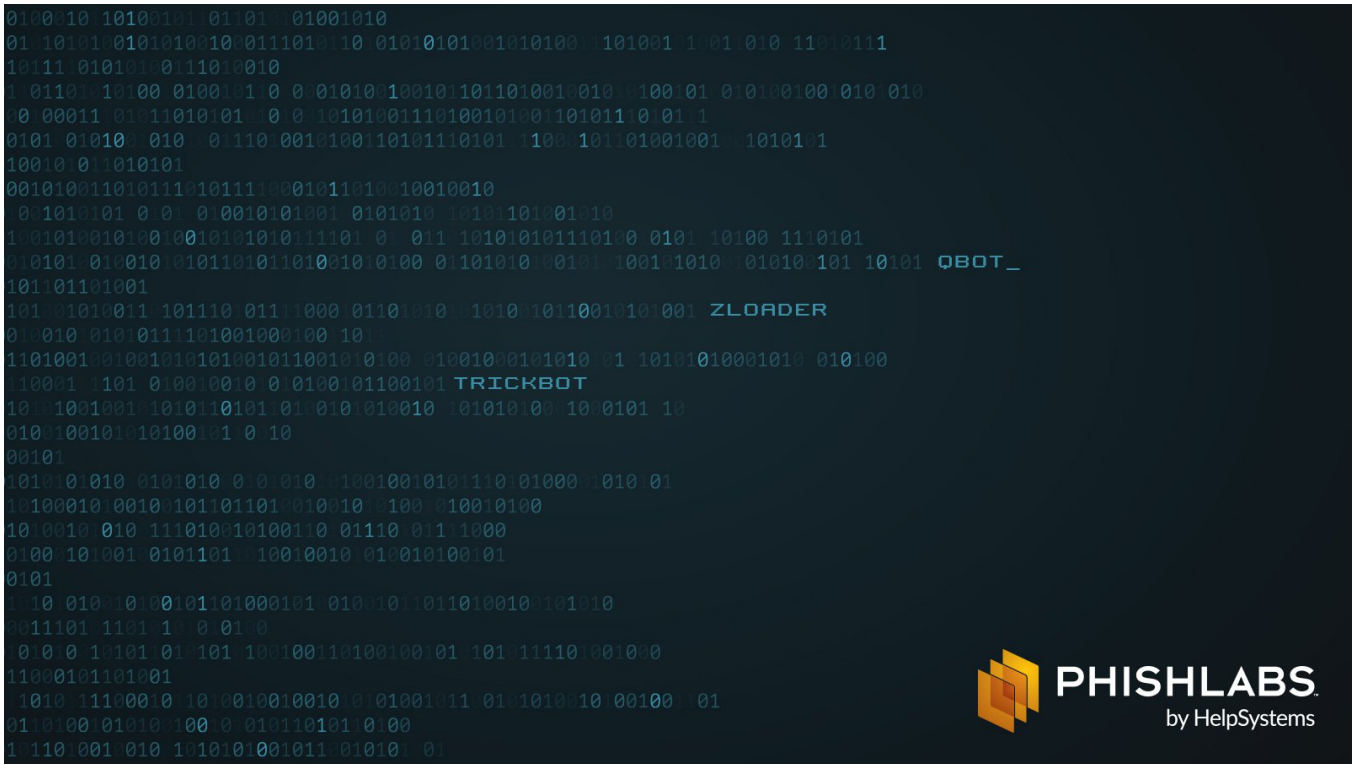
Learn about how PhishLabs helps organizations defend against ransomware risks with Ransomware Protection.

Additional Resources:



Qbot Payloads Dominate Q1

Qbot payloads targeting enterprises contributed to almost three quarters of all email-based malware since the beginning of 2022.



Qbot, ZLoader Represent 89% of Payload Volume in Q4

Qbot and ZLoader payloads targeting enterprises contributed to almost 89% of email-based malware volume in Q4.

Despite their Simplicity, New Emotet Attacks Forecast Threatening Future

PhishLabs has recently observed attacks targeting enterprises with Emotet payloads for the first time since January, when coordinated efforts by authorities to disrupt operations led this family of threat actors to halt activity.