

# UNC2053 Activity Resumes Following Short Hiatus; Campaign Leverages Google and JetBrains Infrastructure to Distribute SPIKEDNOG

Fusion (FS)

Cyber Crime (CC)

December 10, 2020 06:07:00 PM, 20-00025543, Version: 1

## Executive Summary

- On Dec. 10, 2020, Mandiant Threat Intelligence observed a campaign that distributed SPIKEDNOG, a newly identified UNC2053 downloader.
- This campaign leveraged tactics, techniques, and procedures (TTPs) consistent with previously observed UNC2053 operations, including the use of Google Documents, payloads hosted on Google Drive and JetBrains, code-signed payloads, and similar lure themes.
- Additionally, there is evidence to suggest that a campaign distributed the LOUDPOP downloader on Dec. 9, 2020.
- Given the widespread nature of UNC2053 campaigns, this activity is a concern to organizations across all industry sectors.
- UNC2053 campaigns have previously been a precursor for ransomware operations. For comprehensive recommendations for addressing ransomware, please refer to our blog, [Ransomware Protection and Containment Strategies: Practical Guidance for Endpoint Protection, Hardening, and Containment](#), and the linked [white paper](#).

## Threat Detail

### New Version Details

**Version 2, Dec. 29, 2020:** Mandiant Threat Intelligence updated this report to identify the use of a new downloader family, SPIKEDNOG, and to note the likely use of LOUDPOP on Dec. 9, 2020.

On Dec. 10, 2020, Mandiant Threat Intelligence observed a widespread phishing campaign that distributed SPIKEDNOG downloader payloads ([20-00026720](#)). This campaign used tactics, techniques, and procedures (TTPs) consistent with prior operations, including the use of Google Documents, payloads hosted on Google Drive and JetBrains, code-signed payloads, and similar lure themes ([20-00019240](#), [20-00021688](#)). UNC2053 is a cluster of threat activity responsible for the distribution of multiple loader and backdoor combinations that are tracked by other security companies under the names BazarLoader and BazarBackdoor; however, while functionally similar, Mandiant tracks these different loaders and backdoors as distinct malware families ([20-00024041](#)). This campaign represents the first UNC2053 activity observed since early November, signaling the group's return following a month-long hiatus ([20-00022435](#)).

- Phishing emails from this campaign used several generic subjects and lure themes relating to terminations, debits, and office calls commonly seen in prior UNC2053 phishing campaigns.
- Observed emails included a link to a Google Documents PDF, which contained a link to a malicious payload hosted on Google Drive. The documents from this campaign used customer complaint, bonus

report, and employee termination lure themes, which is consistent with prior UNC2053 operations that distributed KEGTAP and SINGLEMALT (Figures 1 and 2).

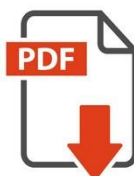
- In one observed infection chain, upon clicking the link contained within the PDF, a SPIKEDNOG downloader payload (MD5: 7a240ae3cf85ad67310c2b307f592012) hosted on the Google Drive was downloaded from the following URL. We also observed evidence that this campaign used JetBrains for payload hosting. Mandiant has previously reported on UNC2053 campaigns that have used both of these platforms in their infection chains ([20-00019240](#), [20-00021688](#)).
  - `hxxps://www[.]google[.]com/url?q=hxxps://drive[.]google[.]com/uc?export%3Ddownload%26id%3D1wSbTEFW0i5NiOeC7YZ23ARLc9rejsSvA&sa=D&ust=1607624297614000&usg=AOvVaw3RxcJWkzJcihfNwtM5CNyq`
- Payloads used in this campaign were signed using a certificate with the common name "OOO Inversum."

While not directly observed in distribution, several LOUDPOP downloader payloads were identified that were compiled on Dec. 9, 2020, one day prior to the SPIKEDNOG payloads (MD5s: fe0c4a65b6460d9163d05815ff3dc40d, 9a8c7ae7424367b8c24d5d70b9c1c867, dac91ccf0929071e9db5b75be0f6a3a6). These LOUDPOP payloads had several hard-coded C&C IP addresses in common with the Dec. 10, 2020, SPIKEDNOG payloads.



## Customer Complaint Report

[12-20](#)



### [EXPAND AND PREVIEW](#)

According to the rules of our company, preview is available only on corporate computers.

If the report doesn't start automatically, [click here](#).

## Employees bonus report

[#12-20/4057](#)

Von [Google Drive](#) veröffentlicht – [Missbrauch melden](#)

Figure 1: Sample complaint-themed Google Documents PDF with malicious links

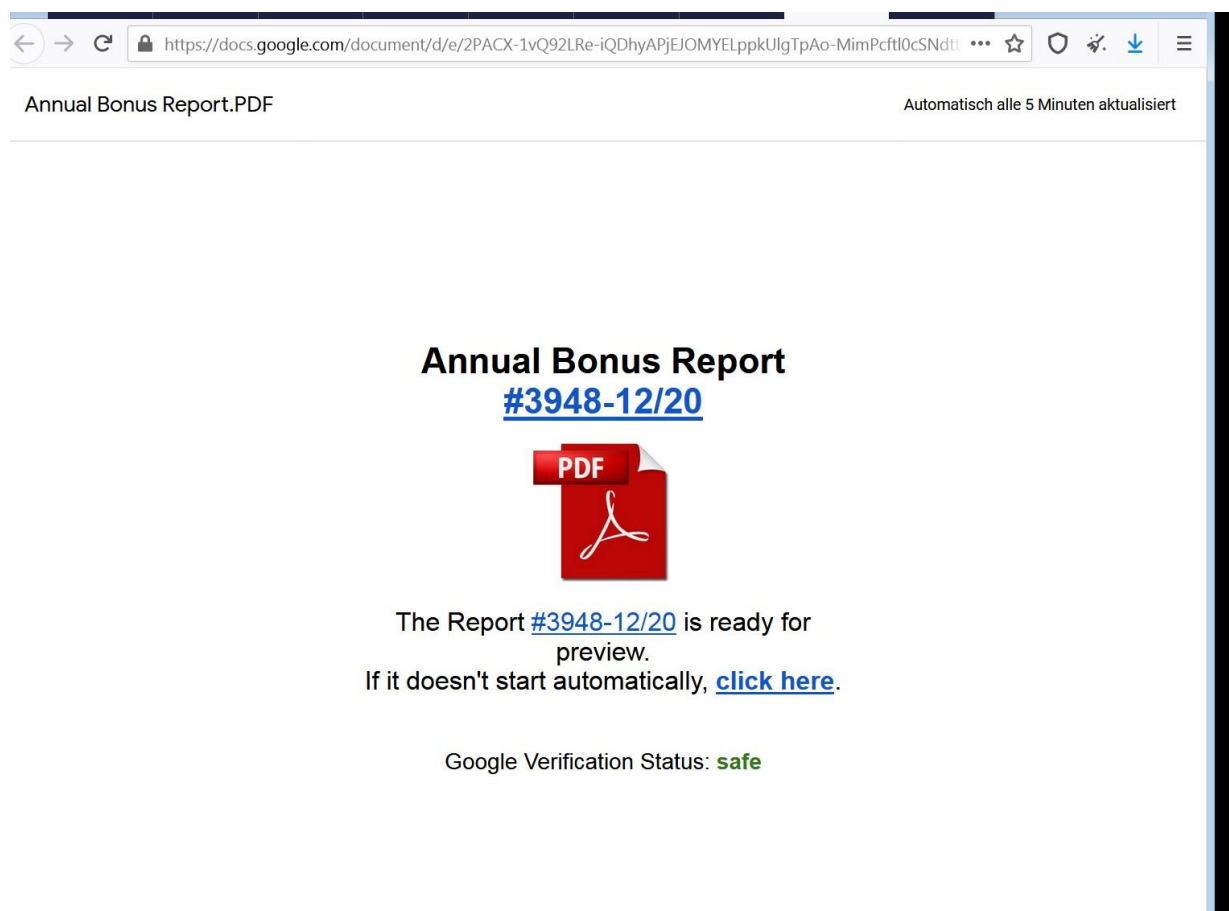


Figure 2: Sample bonus-themed Google Documents PDF with malicious links

## Implications

Mandiant has previously reported on numerous UNC2053 campaigns distributing payloads such as KEGTAP and SINGLEMALT, the development of which we have high confidence is associated with TrickBot-related actors ([20-00007310](#)). While the reason for the hiatus is unclear, there are several possible explanations such as the group shifting to development tasks or taking a planned break. Notably, this campaign involved a new downloader family that we refer to as SPIKEDNOG, providing some evidence that malware development continued over this time frame. Mandiant has previously observed UNC2053 campaigns lead to interactive intrusion activity, which includes the delivery of BEACON and, in at least some instances, the deployment of ANCHOR. This infection chain has frequently led to the post-compromise deployment of ransomware, suggesting it is currently the primary motivation of these campaigns ([20-00022104](#), [20-00019911](#)).

**First Version Publish Date** December 10, 2020

06:07:00 PM



5950 Berkshire Lane, Suite 1600 Dallas, TX

75225

This message contains content and links to content which are the property of FireEye, Inc. and are protected by all applicable laws. This cyber threat intelligence and this message are solely intended for the use of the individual and organization to which it is addressed and is subject to the subscription Terms and Conditions to which your institution is a party. Onward distribution in part or in whole of any FireEye proprietary materials or intellectual property is restricted per the terms of agreement. By accessing and using this and related content and links, you agree to be bound by the subscription .

For more information please visit: <https://intelligence.fireeye.com/reports/20-00025543>

© 2021, FireEye, Inc. All rights reserved.