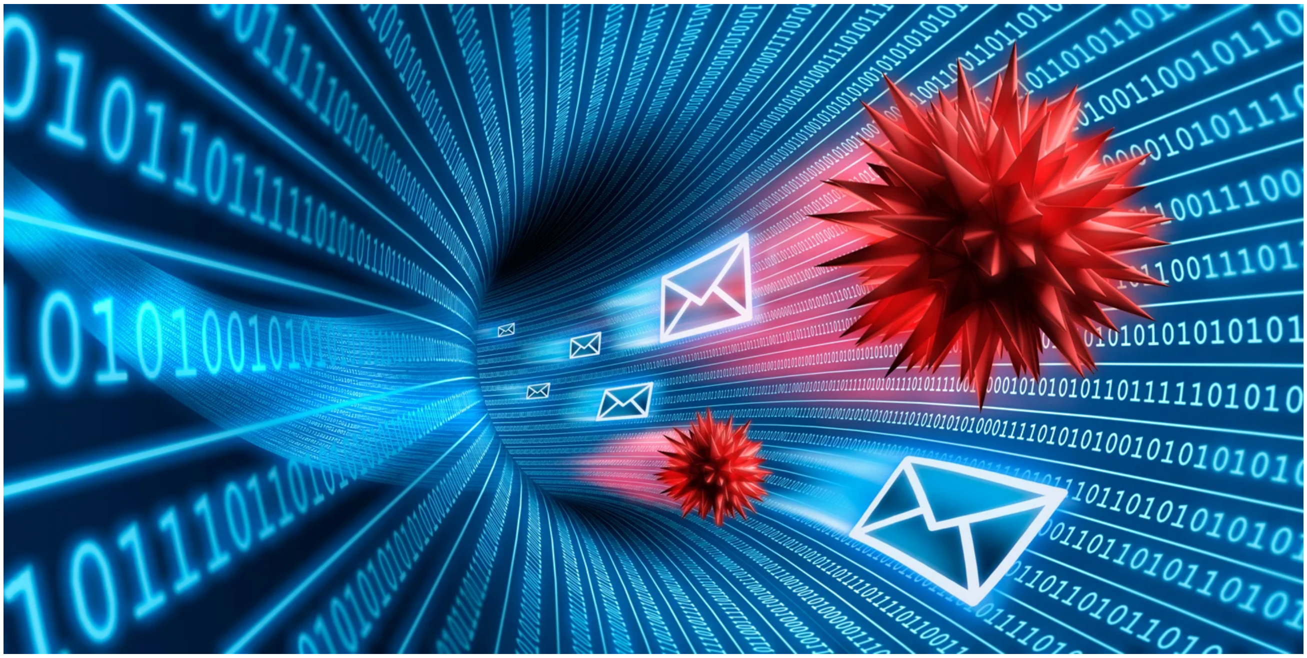
Corporate website contact forms used to spread BazarBackdoor malware

bleepingcomputer.com/news/security/corporate-website-contact-forms-used-to-spread-bazarbackdoor-malware/

Bill Toulas

By
Bill Toulas

- March 10, 2022
- 05:36 PM
- 0



The stealthy BazarBackdoor malware is now being spread via website contact forms rather than typical phishing emails to evade detection by security software.

BazarBackdoor is a stealthy backdoor malware created by the TrickBot group and is now under development by the Conti ransomware operation. This malware provides threat actors remote access to an internal device that can be used as a launchpad for further lateral movement within a network.

The BazarBackdoor malware is usually spread through phishing emails that include malicious documents that download and install the malware.

However, as secure email gateways have become better at detecting these malware droppers, distributors are moving to new ways of spreading the malware.

Contact forms replacing emails

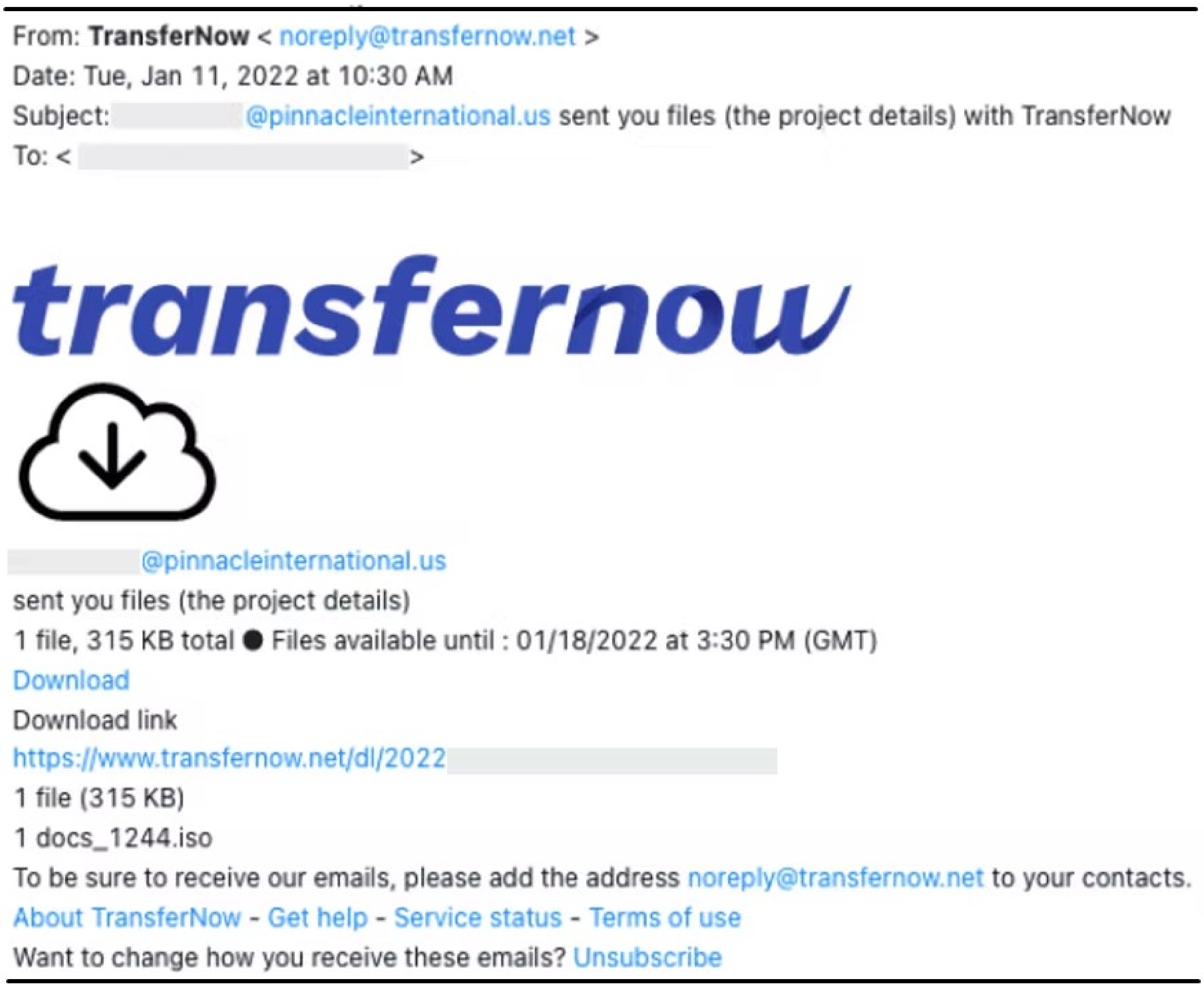
In a new report by Abnormal Security, analysts explain that a new distribution campaign started in December 2021 targets corporate victims with BazarBackdoor, with the likely goal of deploying Cobalt Strike or ransomware payloads.

Instead of sending phishing emails to the targets, the threat actors first use corporate contact forms to initiate communication.

For example, in one of the cases seen by Abnormal's analysts, the threat actors posed as employees at a Canadian construction company who submitted a request for a product supply quote.

After the employee responds to the phishing email, the attackers send back a malicious ISO file supposedly relevant to the negotiation.

Since sending these files directly is impossible or would trigger security alerts, the threat actors use file-sharing services like TransferNow and WeTransfer, as shown below.



From: **TransferNow** < noreply@transfernow.net >
Date: Tue, Jan 11, 2022 at 10:30 AM
Subject: [redacted]@pinnacleinternational.us sent you files (the project details) with TransferNow
To: < [redacted] >

transfernow

[redacted]@pinnacleinternational.us
sent you files (the project details)
1 file, 315 KB total ● Files available until : 01/18/2022 at 3:30 PM (GMT)
Download
Download link
https://www.transfernow.net/dl/2022[redacted]
1 file (315 KB)
1 docs_1244.iso
To be sure to receive our emails, please add the address noreply@transfernow.net to your contacts.
About TransferNow - Get help - Service status - Terms of use
Want to change how you receive these emails? Unsubscribe

Phishing message pointing to a malicious file download *(Abnormal Security)*

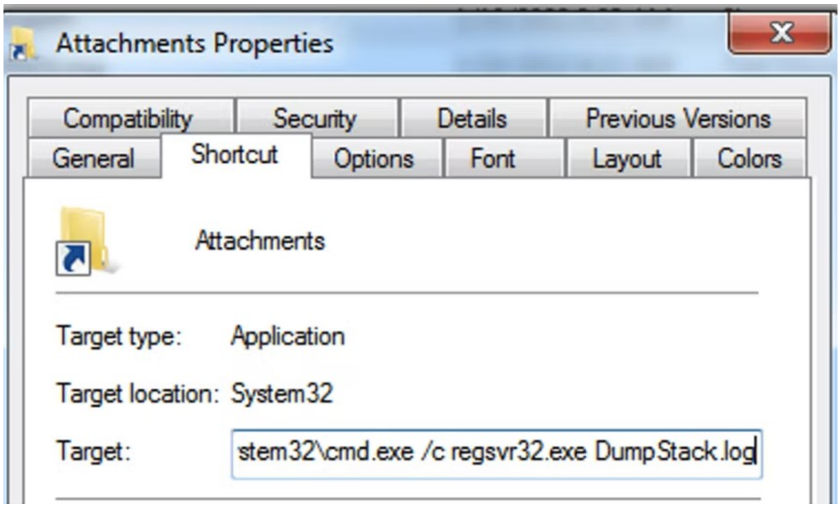
We reported a similar case of contact form abuse in August, where fake DMCA infringement notices sent via contact forms were installing BazarBackdoor.

In April 2021, we also reported on a phishing campaign using contact forms to spread the IcedID banking trojan and Cobalt Strike beacons.

Hiding BazarLoader

The ISO archive attachment contains a .lnk file and a .log file. The idea here is to evade AV detection by packing the payloads in the archive and having the user manually extract them after download.

The .lnk file contains a command instruction that opens a terminal window using existing Windows binaries and loads the .log file, which is, in reality, a BazarBackdoor DLL.



Target type: Application

Target location: System32

Target: stem32\cmd.exe /c regsvr32.exe DumpStack.log

BazarLoader executable posing as a .log file *(Abnormal Security)*

When the backdoor is loaded, it will be injected into the svchost.exe process and contact the command and control (C2) server to receive commands to execute.

Due to many of the C2 IPs being offline at the time of Abnormal's analysis, the researchers couldn't retrieve the second-stage payload, so the ultimate goal of this campaign remains unknown.

Related Articles:

New Bumblebee malware replaces Conti's BazarLoader in cyberattacks

The Week in Ransomware - May 20th 2022 - Another one bites the dust

Conti ransomware shuts down operation, rebrands into smaller units

The Week in Ransomware - May 13th 2022 - A National Emergency

Costa Rica declares national emergency after Conti ransomware attacks

- BazarBackdoor
- BazarLoader
- Cobalt Strike
- Contact Form
- Conti
- Phishing
- Ransomware

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.

- Previous Article
- Next Article

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: