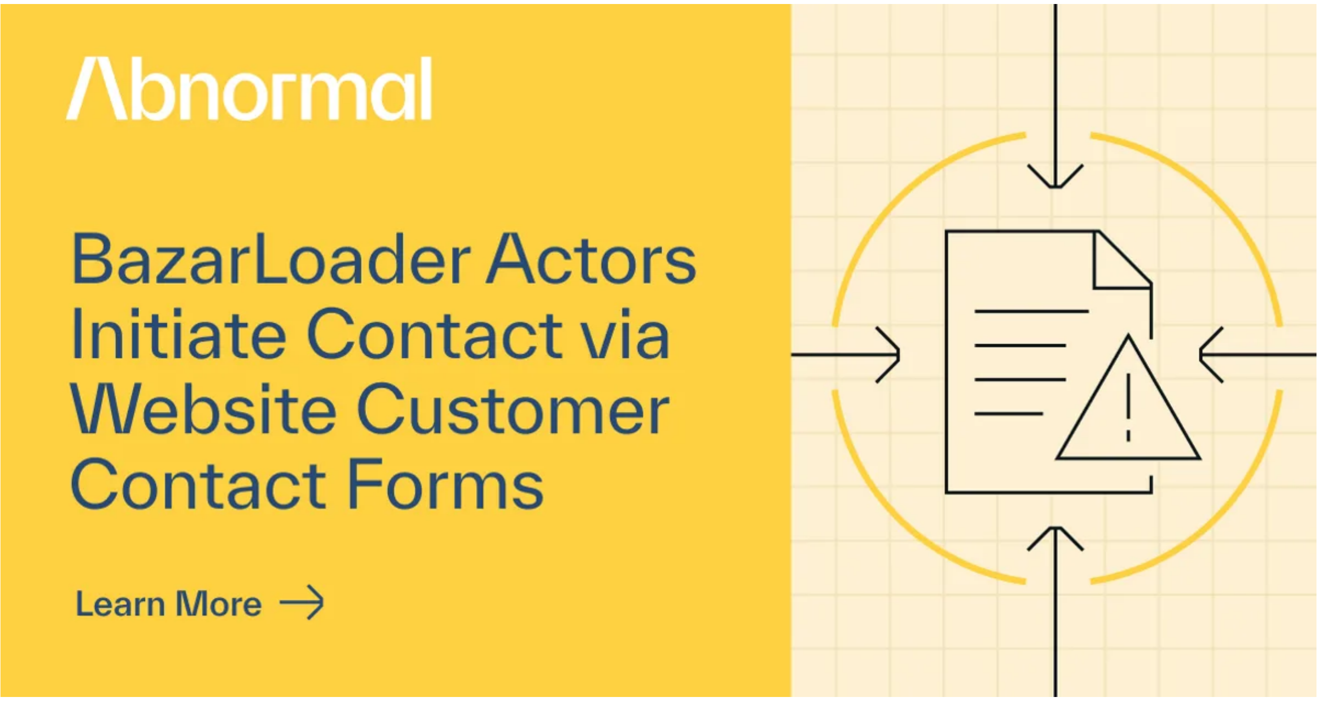
BazarLoader Actors Initiate Contact via Website Contact Forms

abnormalsecurity.com/blog/bazarloader-contact-form


Abnormal
BazarLoader Actors Initiate Contact via Website Customer Contact Forms
Learn More

While most cyberattacks are launched via email, attackers are always looking for new ways to make contact with potential victims. Recently, the threat intelligence team at Abnormal Security observed some attacks targeting our customers that started through an online contact form.

Based on our analysis, we determined that these attacks were attempting to deploy BazarLoader malware. BazarLoader is most closely associated with the cybercrime group known as Wizard Spider, credited with developing the Trickbot banking trojan and Conti ransomware.

Previous BazarLoader campaigns using customer inquiry forms were first identified in 2021, but those attempts used attention-seeking themes to garner artificial urgency. In many cases, the attackers threatened legal action for ongoing copyright violations, with malware disguised as evidence of the misconduct. In these recent campaigns, the actors chose a much lower-impact theme, pretending to be a potential customer in the ordinary course of business.

Attackers Use Online Contact Form to Initiate Communication

Between December 2021 and January 2022, we identified a series of phishing campaigns targeting several of our customers. At first glance, the overall volume of messages seemed low; however, as we continued researching these attacks, it became clear that the volume was artificially deflated because email was not the initial communication method used.

Rather than directly sending a phishing email, the attacker in these cases initiated a conversation through an organization’s website contact form. In these initial contact form submissions, the attacker posed as an employee at a Canadian luxury construction company looking for a quote for a product provided by the target.

There are two primary purposes for choosing this method for initial communication.

1. It disguises the communication as a request that could be reasonably expected to be received through an online request form.
2. It circumvents potential email defenses since the request would be delivered through a legitimate sender and does not contain any malicious content.

Once the contact form request has been submitted by the attacker, they simply wait until someone at the target company reaches out to them to follow up. From the perspective of an email system, the target company is initiating conversation with the attacker rather than the other way around.

After Successful Contact, Attackers Send a Malicious File

After fully establishing their cover identity via email, the threat actors continued project negotiations in an effort to convince their victim to download a malicious file. Often this involved some level of social engineering to find a download method not blocked by the victim’s security protocols, without arousing their suspicion.

Attacker establishing their cover identity via email.

We’ve observed the attacker in these campaigns use two different file sharing services—TransferNow and WeTransfer—to try to deliver the malicious file to victims. If delivery fails using one of these methods, the attacker simply tries again using the other.

Link to TransferNow to download the malware.

BazarLoader Malware Analysis

The file shared by the threat actor is an .iso file with two components, both masquerading as a different file type. At first glance, the .iso file appears to contain a shortcut to the folder with the project and a .log file bearing the name of a legitimate Windows file as an anti-detection technique. In actuality, the two are a windows .lnk file and a .log file that is not DumpStack.log.

Malware sent via TransferNow.

Because shortcut .lnk files allow their creator to specify command-line arguments to perform an action on the victim's device, cybercriminals can use them for nefarious means.

Components of the ISO file.

In this case, the .lnk file properties contain a command instruction to open a terminal window using regsvr32.exe to run the so-named file DumStack.log. In reality, it's a BazarLoader Dynamic-link library (DLL) file.

With a process injection technique, the DLL uses svchost.exe service to evade detection and establish a connection with their command and control (C2) server at the IP address 13.107.21[.]200 using port 443.

svchost.exe process.

Connection established with C2.

Connection established using port 443.

At the time of this investigation, some of the C2 IP addresses were down, and the others were not able to download the second stage of the attack. This leaves some level of uncertainty as to the intended second stage malware payload. However, past relationships between the IP address 13[.]107[.]21[.]200 illustrated in red in the graph below reveal previous links to malware.

Threatcrowd Graph

Malware previously related to the IP address 13[.]107[.]21[.]200 has included the following:

Based on this, it's clear that the threat actors were attempting to execute a multi-stage attack with BazarLoader as a first step.

The BazarLoader Bottom Line

The actors in this campaign attempted to improve their credibility by using customer contact forms to establish their identity as a trusted sender. Then, they sent emails from spoofed domains to impersonate a known business. These spoofed domains were difficult to detect given that they are identical to the legitimate website other than the top-level domain, which was changed from .com to .us to trick users.

After infecting their victim with the dropper malware BazarLoader, the trail unfortunately goes cold. However, we can make some educated guesses as to what they intended to happen next. BazarLoader is usually the first stage in a more sophisticated, multi-stage malware attack, often used to deploy Conti ransomware or Cobalt Strike, for example.

These tools, used separately or in conjunction, help threat actors penetrate networks. At that point, the possibilities for chaos are myriad. Consequences range from unauthorized payments and fund dispersals to total system shutdown and even persistent long-term network intrusion.

To learn more about how Abnormal can stop these attacks before they reach you, request a demo of the platform.

Indicators of Compromise (IOCs)

104[.]215[.]148[.]63

45[.]15[.]131[.]126

148[.]163[.]42[.]203

45[.]41[.]204[.]150

193[.]169[.]86[.]84

76[.]6[.]231[.]20

131[.]253[.]33[.]200

72[.]21[.]91[.]29

docs_1244.iso
97806F6DA402F135FA0556ADF5809D6D3BC629E967A0771B9FEB5BA55267D560

DumpStack.log
8395B26BE4A7D57F9B60839257C3E7B9E6756DBBEB818DE6575987D6E041C8FD

Attachments.lnk
CE6E63191588E449DE4AB45FF4D32E1BBD1C67681C74C32DE3A4DB63331278CC