Wrapping Up a Year of Infamous Bazar Campaigns

By Avigayil Mechtinger

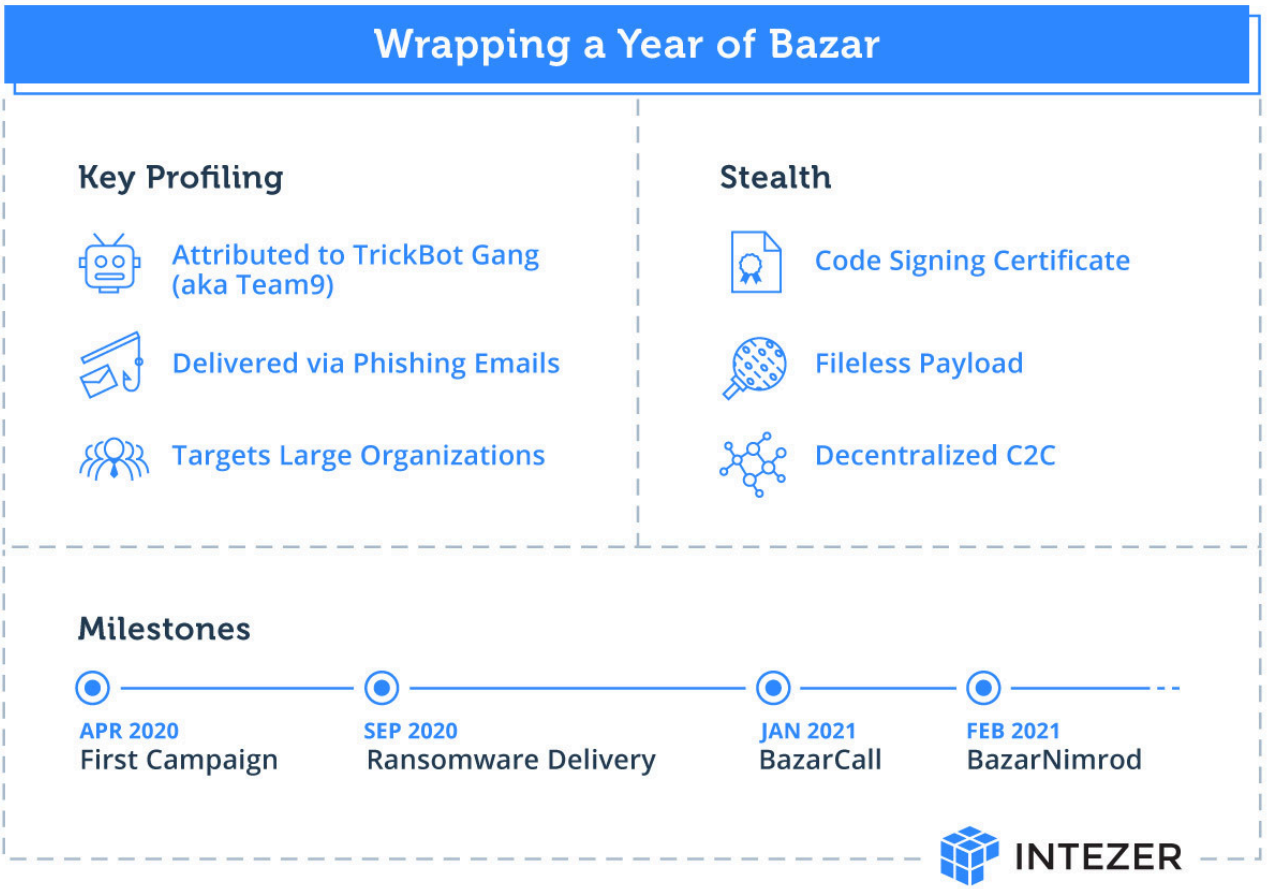
Published: 2021-05-27 · Archived: 2026-04-05 13:55:50 UTC

Bazar is the latest tool developed by the TrickBot gang

Common malware used for cybercrime such as Agent Tesla, Dridex and Formbook have been around for at least five years and are still distributed and active. About one year ago, a new malware named **Bazar** breathed some fresh air into this landscape. Since its first campaign, Bazar has been extremely active and has taken part in large-scale breaches including the nationwide Ryuk ransomware attack on UHS hospitals.

The name 'Bazar' was given to the malware because of its use of EmerDNS (.bazar) domains for command-and-control networking. On top of serving as a backdoor, Bazar is designed to gain a foothold on the victim's machine to deliver an additional payload as a next phase of the attack. The time between Bazar installation and payload delivery can vary between a few hours to days.

In this post we will profile Bazar and highlight four prominent campaigns delivering this year-old malware.



Key Profiling

Attribution

Based on code similarities, delivery, infrastructure and operation methods, researchers believe that Bazar was developed by the TrickBot gang (aka Team9).

Targets

The operators behind the malware are mainly financially motivated, meaning they target organizations with high capital.

Delivery Method

The malware delivery method is purely based on social engineering initiated with a phishing email. The email will usually contain a link to a website, hosting a malicious Microsoft Office document, delivering Bazar upon running the document on a victim's machine, or it will host the malware itself masqueraded as a document.

Stealth

Bazar implements the following evasion techniques to bypass detection:

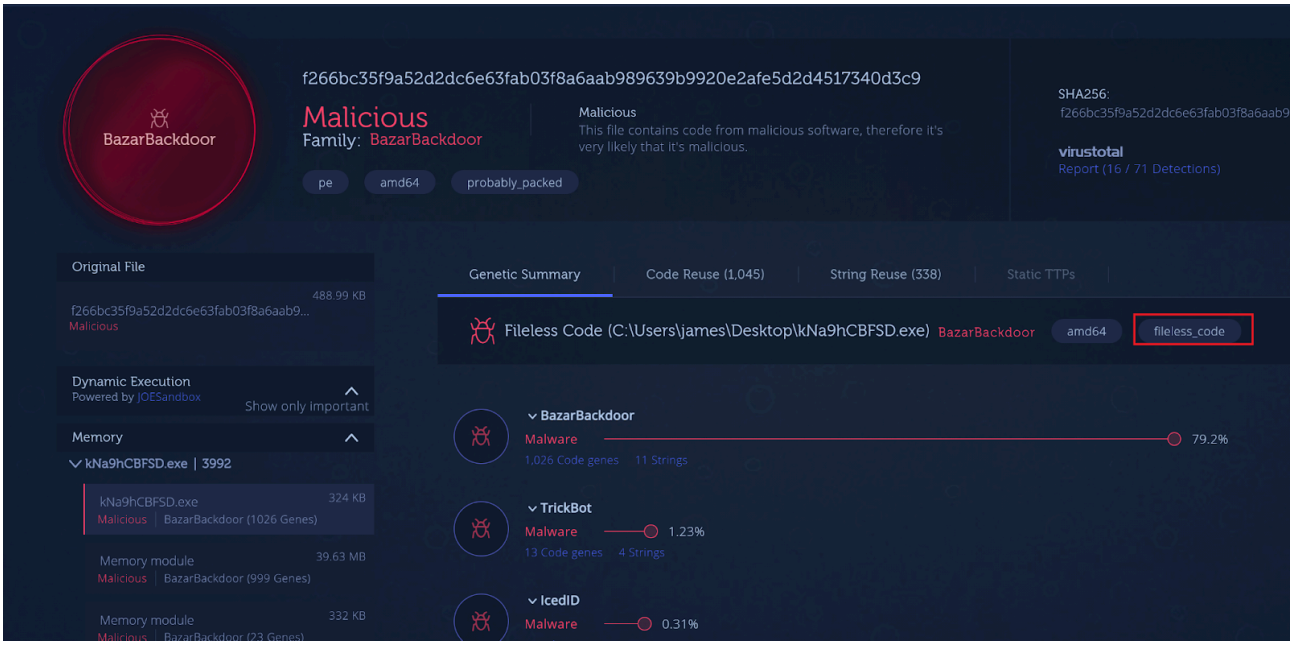
Signing malware with certificates

: Antiviruses tend to rely on code signing certificates to increase the credibility of a file. Therefore, signed files are less likely to be detected as malicious by Antivirus vendors.

Signed Bazar files were fully undetected in VirusTotal

Fileless payload

: Bazar uses a lightweight loader to inject its fileless payload into memory. Fileless malware challenges traditional Antivirus solutions as it resides only in memory and leaves no footprint on disk. The following is the genetic analysis of a Bazar sample (3578e96b72cba790179d546f11e045ca) injecting fileless code into memory.



Bazar sample (3578e96b72cba790179d546f11e045ca) injects fileless code

Use of decentralized C2C

: For its C2C communication, Bazar uses EmerDNS which is a decentralized domain name system based on Emercoin blockchain technology. EmerDNS domains cannot be altered, revoked, or suspended, which allows Bazar's operations to be nearly immune from a take down attempt by law enforcement.

Timeline and Milestone Campaigns

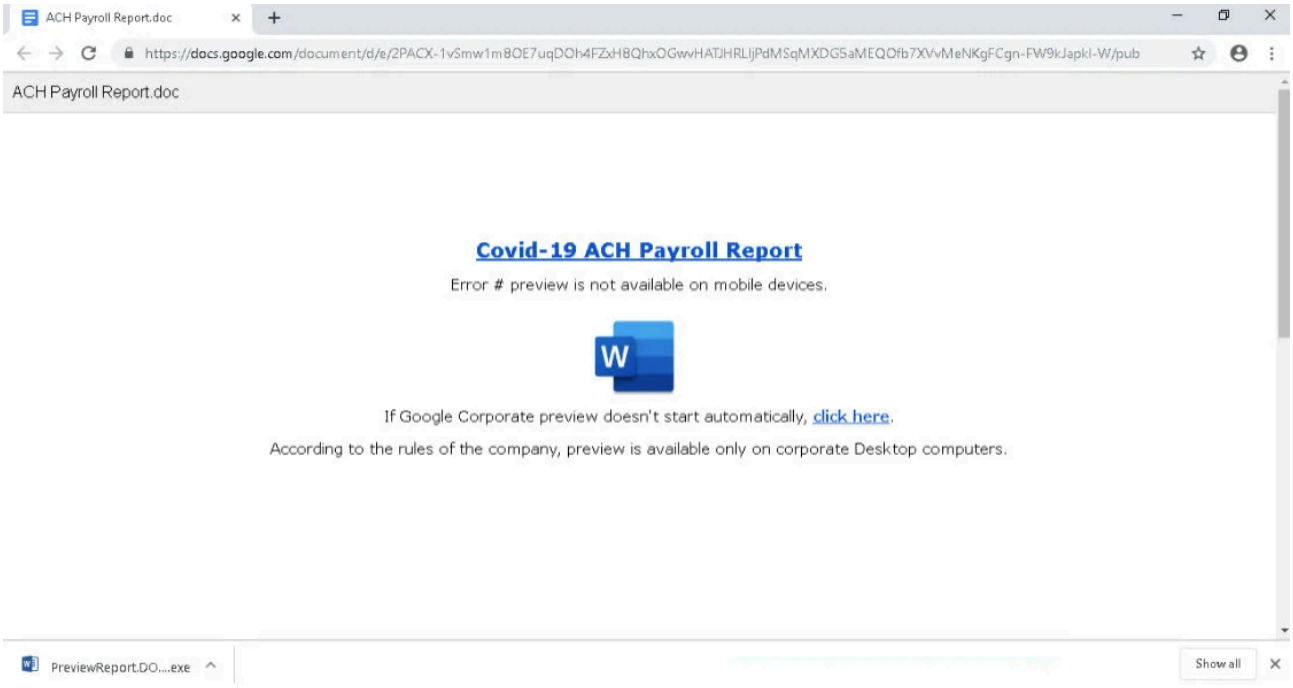
As Bazar evolves and takes part in different phishing campaigns, we are highlighting the top four milestones of this threat so far.

Apr 2020 – Bazar Exposed to the Masses

With the outburst of COVID-19, many threat actors leveraged the pandemic for phishing campaigns. This theme was used as part of the first documented campaign delivering Bazar.

Similar to other campaigns using Bazar, this one began with a phishing email containing a link to a page hosted on Google Docs. On this page, the victim was lured to click on a link preview to a doc report. By clicking on the link, the victim would download the Bazar malware executable masqueraded as a document. Because Windows does not present a file's extension by default, threat actors are able to trick victims by masquerading a non-executable file type, so that the file has a word document icon but it is in fact an executable.

The next image shows a Google Docs page hosting the malware executable.



COVID-19 themed phishing campaign (source: [BleepingComputer](#)) Interestingly, one of these phishing emails was sent to a BleepingComputer domain.

Bazar targeting BleepingComputer domain

Sep 2020 – Healthcare, Ransomware and Bazar in Between

UHS hospitals were hit by a Ryuk ransomware attack in September 2020. This attack was part of a greater trend targeting hospitals and other healthcare-related organizations in the United States.

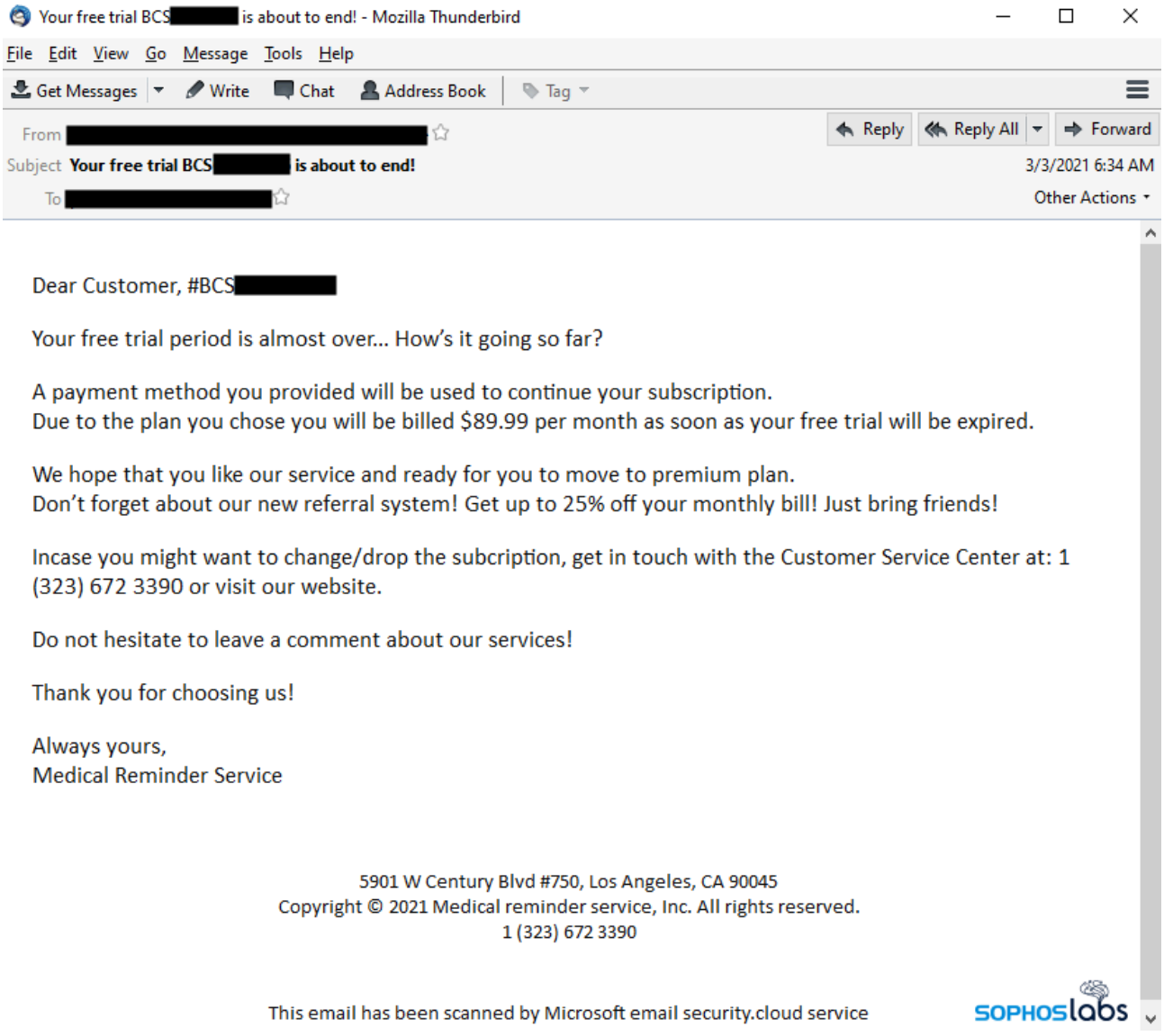
These ransomware attacks were initiated with phishing emails sent to employees delivering Bazar but also BuerLoader or TrickBot. After an employee was lured to install Bazar, a Cobalt Strike Beacon was delivered to the victim's machine for lateral movement and persistence. Together with Cobalt Strike, other penetration testing tools were installed and ran on the victim's machine for reconnaissance and privilege escalation purposes. Ryuk ransomware was delivered as the final step of the attack to run widely on the organization's assets.

CISA alert on the ransomware campaign This attack chain not only targeted the healthcare sector but also went after different organizations inside France after it became public that Sopra Steria, a French consulting organization, was hit by Ryuk.

Jan 2021 – Hello, Who is This?

The **BazarCall** campaign may be the most interesting social engineering method used for delivering Bazar thus far.

As the first step, a personalized phishing email is sent claiming that a free trial for a [fake] product is about to expire, and the addressee will be charged via a “pre provided payment method.” The email also states that if the addressee wishes to drop the subscription, they can make a call to the “customer service center.” Once a victim calls the customer service center number, the “service provider” lures the user to browse a phishing website, insert a code, and click on “unsubscribe.” By clicking unsubscribe a malicious Microsoft Office document is downloaded delivering Bazar.



Example of a BazarCall phishing email (source: Sophos) The email has no indication of maliciousness as it does not contain any links or attachments but it is purely an attempt to exploit the innocence of the victims who are lured to make the phone call.

This YouTube video documents a phone call between a researcher posing as a victim and the "service provider."

The campaign, which started by delivering BazarLoader, continues to deliver other loaders such as IceID.

Feb 2021 – Nim What?

In the beginning of February, a new and unusual version of Bazar was detected—an implementation of the backdoor written in Nim, which is a statically-typed self-contained programming language.

Because Nim is not a common choice for malware development, it is believed that the use of this programming language is an attempt to bypass detection. This attempt can be considered successful as this version, also known as 'BazarNimrod' and 'NimzaLoader,' had low detection rates in VirusTotal.

Bazar written in Nim with low detection rate in VirusTotal

Bazar is not the first malware written in Nim. Sofacy (Russian APT) developed a downloader in Nim for their Zebrocy tool.

Final Words

Threat actors are highly motivated and must keep reinventing themselves to stay effective. They put in the time and money to bypass Antivirus detection on the way to successful compromises. We assess that cybercriminals will continue to step up their game with social engineering creativity and different malware implementation.

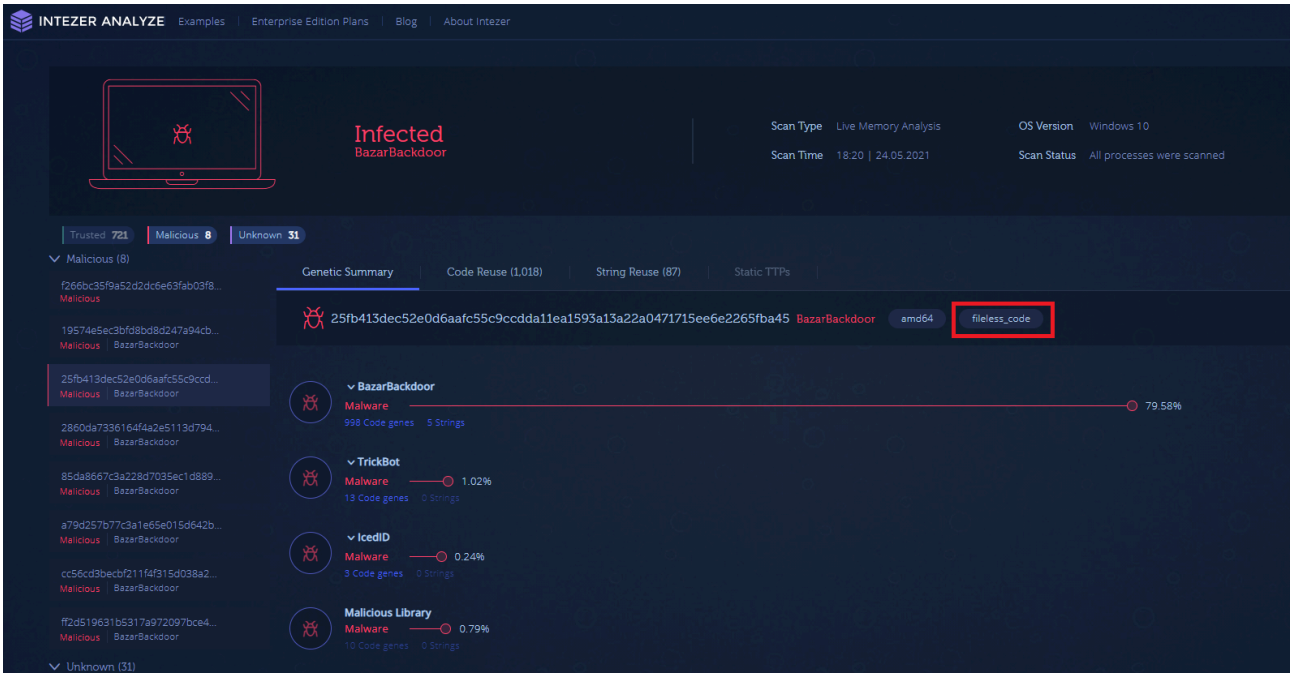
How to Protect Your Organization

Bazar and similar threats use social engineering as an entry point and keep a low profile once inside. Keep in mind that it takes only one employee to take down an entire organization.

Take the following steps to keep your organization clean from these type of attacks

:

- Enhance social engineering awareness inside your organization.
- Perform proactive hunting on all endpoints inside your organization to make sure that no traces of malicious code or malware exist. Intezer's live Endpoint Scanner collects all binaries running in memory, including **fileless**, and classifies them using genetic code analysis technology.



Endpoint scan on an infected machine

References

- https://www.bleepingcomputer.com/news/security/bazarbackdoor-trickbot-gang-s-new-stealthy-network-hacking-malware/

- https://www.bleepingcomputer.com/news/security/bazarcall-malware-uses-malicious-call-centers-to-infect-victims/
- https://www.advanced-intel.com/post/front-door-into-bazarbackdoor-stealthy-cybercrime-weapon
- https://threatpost.com/bazarloader-malware-slack-basecamp/165455/
- https://news.sophos.com/en-us/2021/04/15/bazarloader/
- https://www.cybereason.com/blog/a-bazar-of-tricks-following-team9s-development-cycles#trickbot-connection
- https://www.advanced-intel.com/post/front-door-into-bazarbackdoor-stealthy-cybercrime-weapon

---