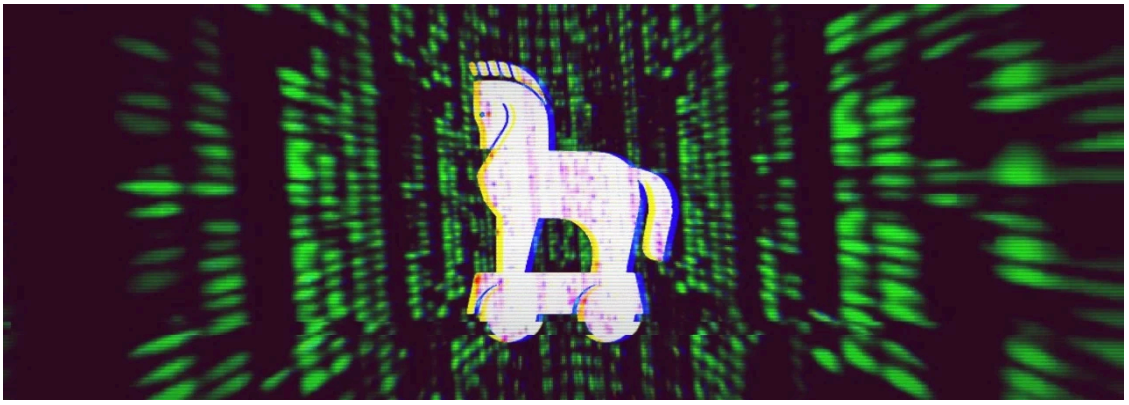
BazarBackdoor: TrickBot gang’s new stealthy network-hacking malware

By Lawrence Abrams

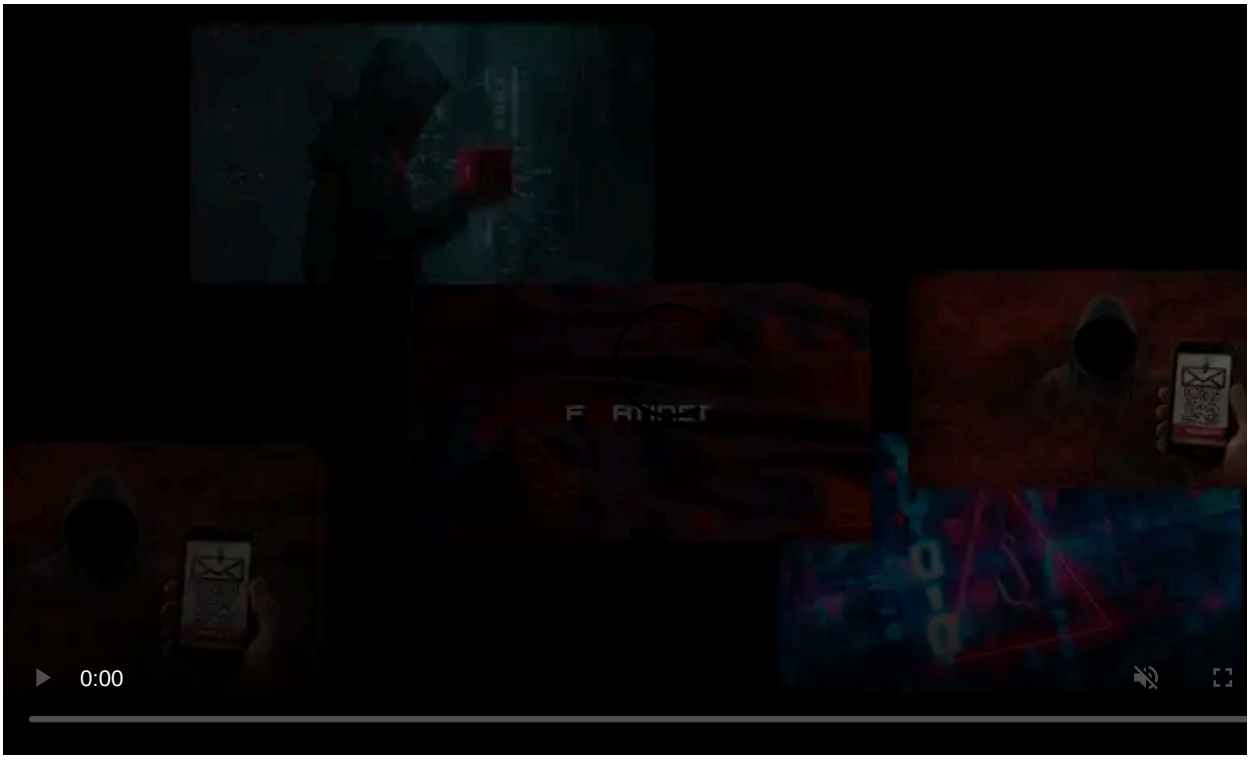
Published: 2020-04-24 · Archived: 2026-04-05 22:23:13 UTC

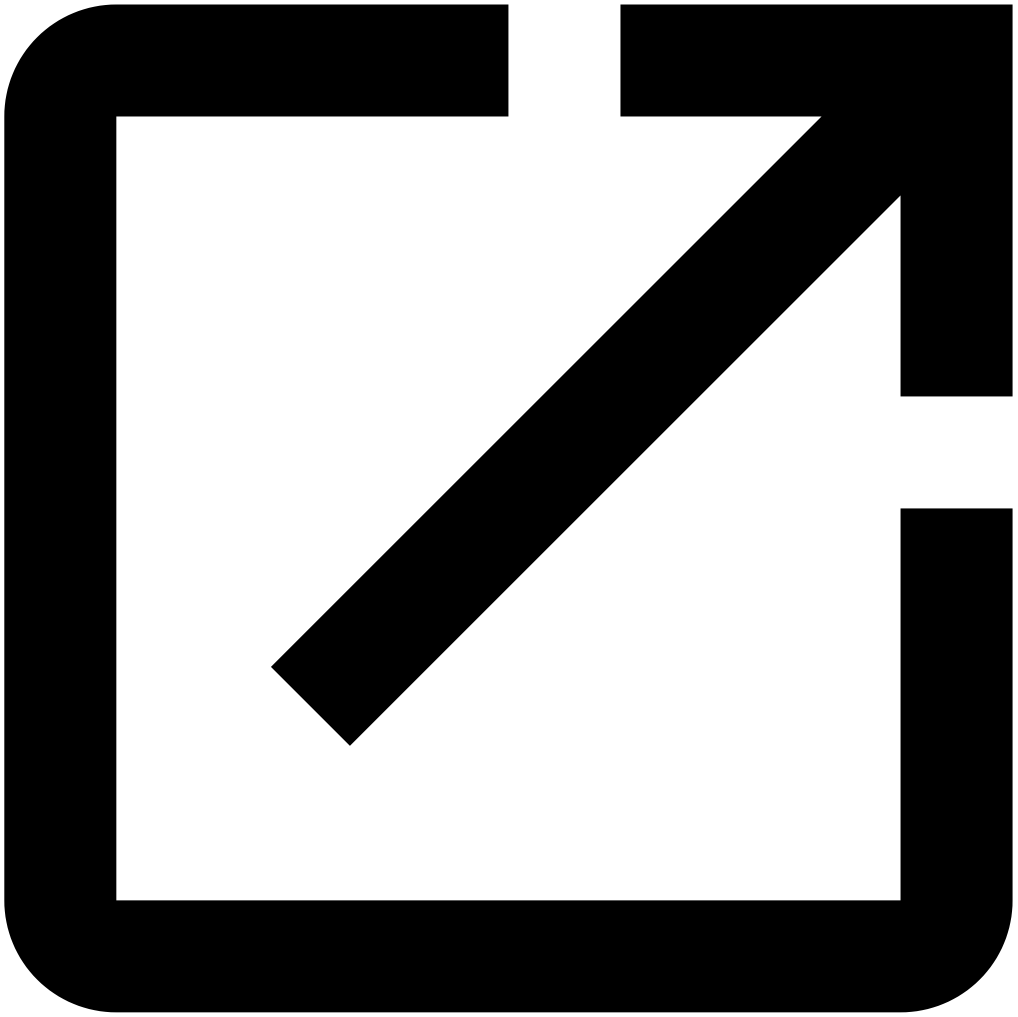


A new phishing campaign is delivering a new stealthy backdoor from the developers of TrickBot that is used to compromise and gain full access to corporate networks.

In advanced network attacks such as enterprise-targeting ransomware, corporate espionage, or data exfiltration attacks, quietly gaining access to and control over a corporate network is a mandatory step.

In new phishing attacks discovered over the past two weeks, a new malware named 'BazarBackdoor', or internally by the malware developers as simply "backdoor", is being installed that deploys a network-compromising toolkit for the threat actors.

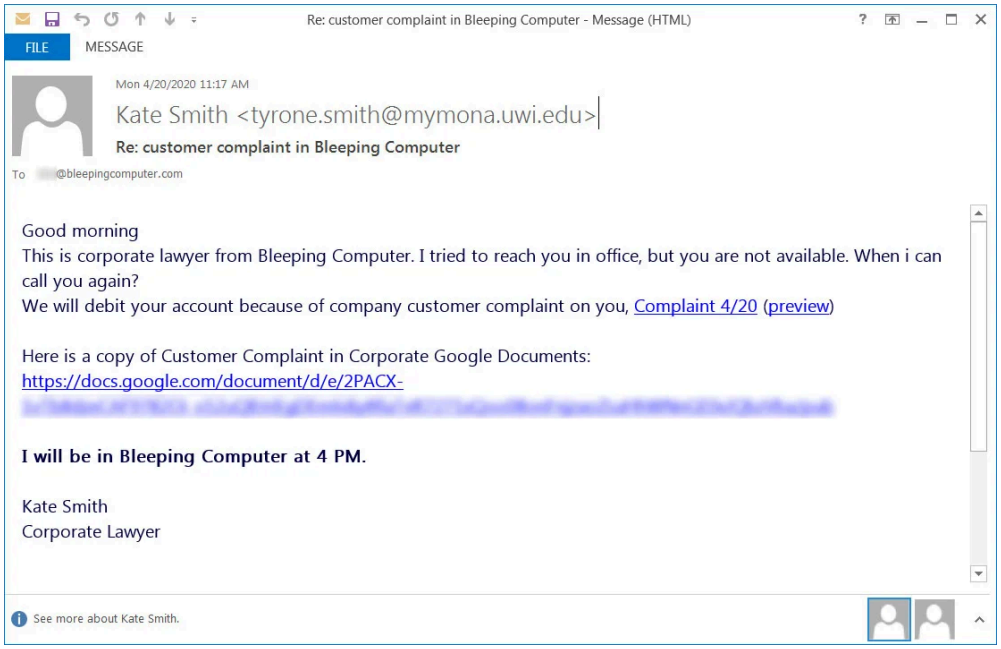

0:00



The developers of the infamous TrickBot trojan are believed to be behind this new backdoor due to code similarities, executable crypters, and its infrastructure.

The attack starts with a phishing email

The initial attack starts with phishing campaigns that utilize a wide variety of lures such as customer complaints, COVID-19 themed payroll reports and employee termination lists that contain links to documents hosted on Google Docs.



Example BazarLoader phishing email

When sending the phishing emails, the attackers are utilizing the Sendgrid email marketing platform.

```
Received: from o2.hv1e.shared.sendgrid.net (o2.hv1e.shared.sendgrid.net. [167.89.100.166])
        by mx.google.com with ESMTPS id o25si511895ejh.73.2020.04.20.07.23.51
        for <                                                    >
        (version=TLS1_3 cipher=TLS_AES_128_GCM_SHA256 bits=128/128);
        Mon, 20 Apr 2020 07:23:52 -0700 (PDT)
```

Sent via Sendgrid

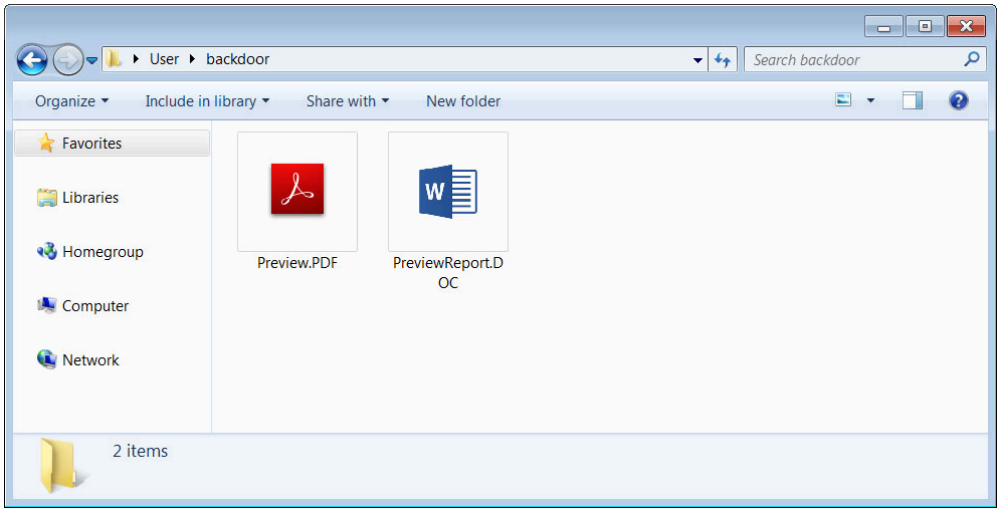
Unlike many phishing attacks, this campaign is putting a lot of thought into their creatives by stylizing their landing pages to correspond to the lures, or themes, of the emails.

For example, as you can see below, we have one landing page utilizing a COVID-19 Payroll Report template while another pretends to be a customer complaint from a corporate lawyer.

Each of the landing pages pretends to be a Word document, Excel spreadsheet, or PDF that cannot be properly viewed and prompts the user to click on a link to properly view the document.

When the link is clicked, an executable will be downloaded instead that uses an icon and name associated with the icon shown on the landing page.

For example, the 'COVID-19 ACH Payroll Report' theme will download PreviewReport.DOC.exe, while the "Customer Complaint" theme will download Preview.PDF.exe.



BazarLoader executables

As Windows does not display file extensions by default, most users will see "Preview.PDF" or "PreviewReport.DOC" and open them thinking they are legitimate Word and PDF documents.

This executable is the loader for the backdoor and, according to security researcher James, is being called "BazaLoader".

Once launched, the backdoor will be stealthily installed on the computer.

Attachment stealthily loads fileless backdoor

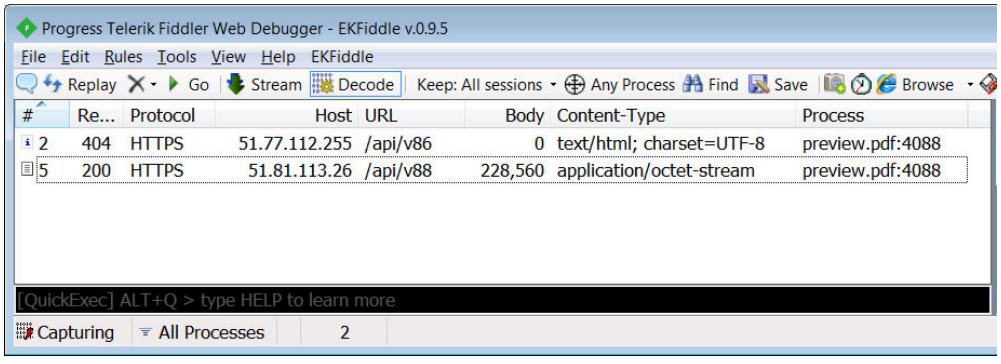
After a victim launches the downloaded file, the loader will sleep for a short period of time and then connect to command and control servers to check-in and download the backdoor payload.

To get the address of the command and control servers, BazarLoader will use the Emercoin decentralized DNS resolution service to resolve various hostnames that use the 'bazar' domain. The 'bazar' domain can only be utilized on Emercoin's DNS servers, and as it is decentralized, it makes it difficult, if not impossible, for law enforcement to seize the hostname.

The hostnames used for the command and control servers are:

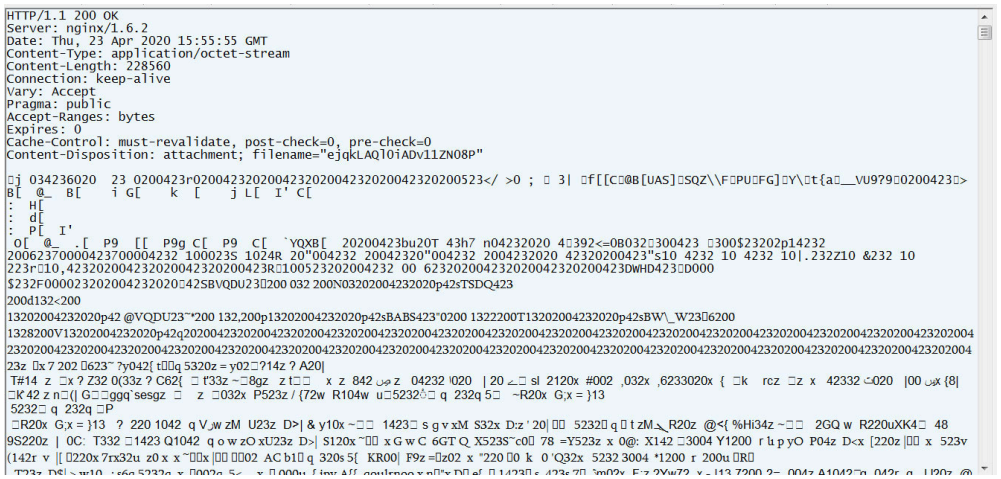
```
 forgame.bazar
bestgame.bazar
thegame.bazar
newgame.bazar
portgame.bazar
```

Once the IP address for the command and control server is resolved, the loader will first connect to one C2 and perform a check-in. In our tests, this request always returned a 404 HTTP error code.



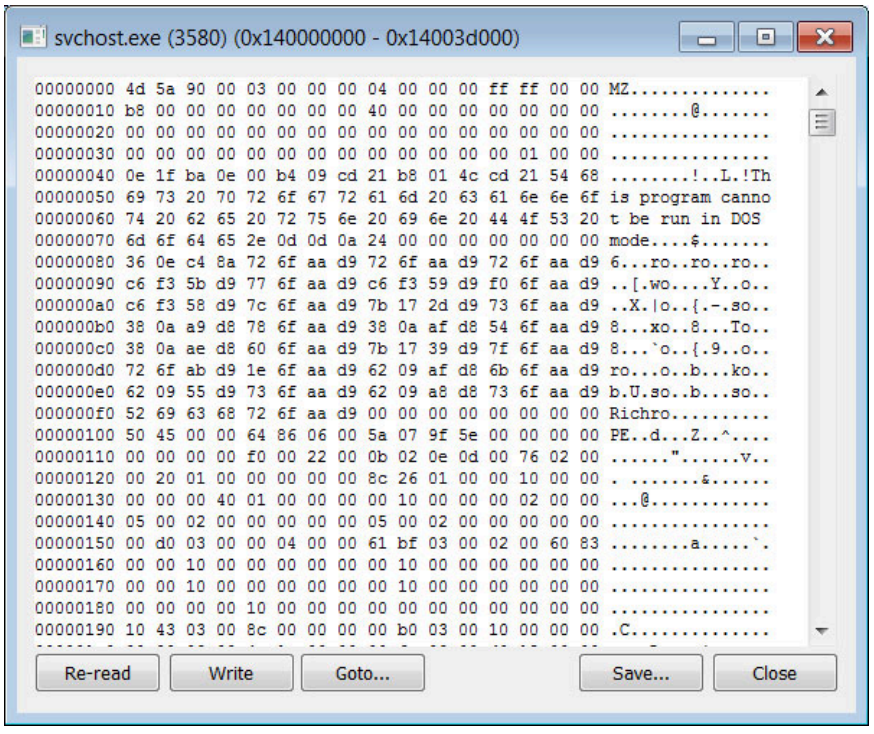
Command and control server communication

The second C2 request, though, will download a XOR encrypted payload, which is the BazarBackdoor backdoor malware.



XOR encrypted payload

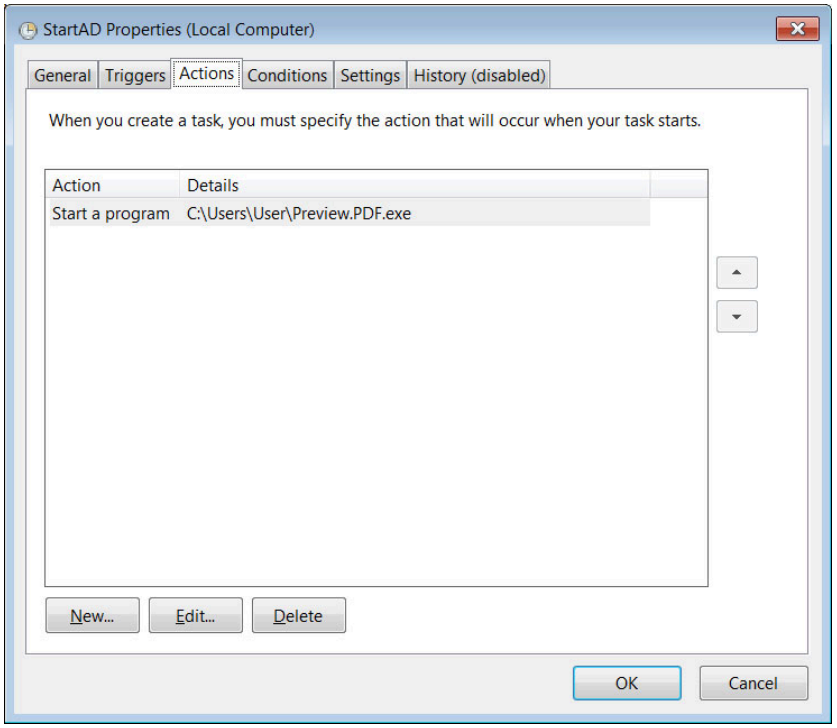
After the payload is downloaded, it will be filelessly injected into the C:\Windows\system32\svchost.exe process. Security researcher Vitali Kremez, who has published a technical report, told BleepingComputer that this is done using the Process Hollowing and Process Doppelgänging techniques.



Injected backdoor into svchost.exe

As Windows users have grown numb to svchost.exe processes running in Task Manager, one more svchost process is not likely to arouse suspicion for most users.

A scheduled task will also be configured to launch the loader when a user logs into Windows, which will allow new versions of the backdoor to be routinely downloaded and injected into the svchost.exe process.



Scheduled task

After a period of time, both Kremez and James have told BleepingComputer that the backdoor will download and execute the Cobalt Strike penetration testing and post-exploitation toolkit on the victim's machine.

Cobalt Strike is a legitimate cybersecurity application that is promoted as an "adversary simulation platform" intended to perform network security assessments against a simulated advanced threat actor persisting in a network.

Attackers, though, commonly use cracked versions of Cobalt Strike as part of their toolkit when spreading laterally throughout a network, stealing credentials, and deploying malware.

By deploying Cobalt Strike, it is clear that this stealthy backdoor is being used to gain footholds in corporate networks so that ransomware can be deployed, data can be stolen, or to sell network access to other threat actors.

Strong ties to the developers of Trickbot

Kremez and James have told BleepingComputer that this malware is enterprise-grade and is likely developed by the same group behind the TrickBot trojan.

"This is another high-profile project developed by the same core team as TrickBot due to the spam origin, method of operation, and code overlap analysis," Kremez told BleepingComputer in conversation.

Both the BazarBackdoor and Trickbot utilize the same crypter and email chain deliverables as previous TrickBot campaigns.

Kremez also told us that the TrickBot Anchor project also uses the Emercoin DNS resolution service for command & control server communication.

To further tie the two malware together, James told BleepingComputer that the malware's command and control server's TLS communications had been seen using certificates created in the same manner that historic TrickBot certificates have been created.

Based on the volume of phishing emails being sent out using this new loader/backdoor, BazarBackdoor poses a grave threat to corporate networks that could easily be used to deploy ransomware or perform other attacks.

Businesses should immediately be on the lookout and warn employees of emails coming from sendgrid.net that contain links that download files to prevent their employees from being infected.

Update 4/26/20: Added link to Vitali Kremez's technical report on BazarBackdoor.

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