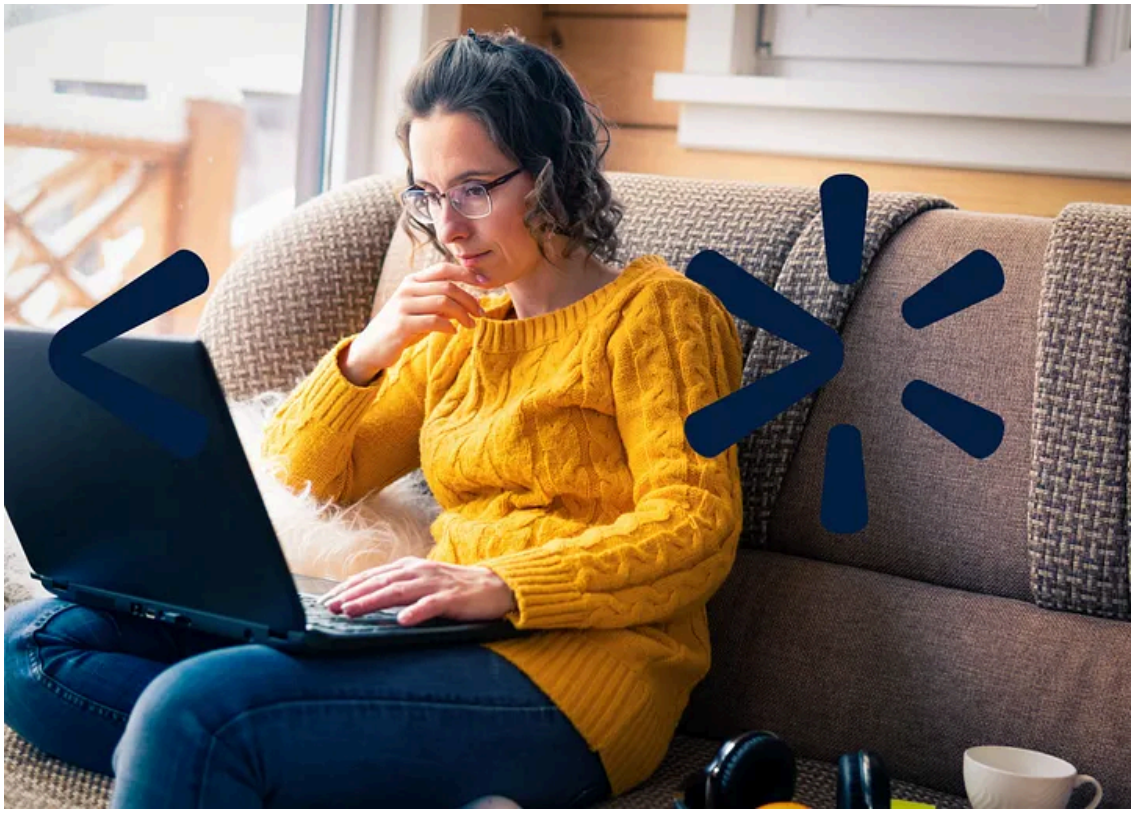
BuerLoader Updates

By Jason Reaves

Published: 2021-05-05 · Archived: 2026-04-05 14:37:04 UTC

By: Joshua Platt and Jason Reaves

Press enter or click to view image in full size



Executive Summary

- Buer task includes domain profiler that appears to have code reuse with the version of Buer being leveraged by TrickBots crew
- Buers new functionality around loading shellcode[4] as a task allowing for broader functionality against targets without the need for downloading a separate CobaltStrike stager
- Buers new panel also includes functionality for helping setup distribution for spamming operations and creation of pre-loader objects

One of the crews involved in TrickBot has been utilizing Buer[1] loader for sometime now[2,5] to ultimately deliver CobaltStrike[3] and ultimately leading to ransomware. The version of Buer being leveraged for these

campaigns has more updates being done to it that appear to be completely designed around an enterprise focus. One such piece that hasn't been discussed very publicly is that Buer also has a component that is frequently delivered in memory as a task and communicates with the same C2 as Buer but over a different port.

DomainInfo

Enter Buers 'DomainInfo' component which is ultimately designed to profile some information about the infected system and the network that it is joined to.

Get Jason Reaves's stories in your inbox

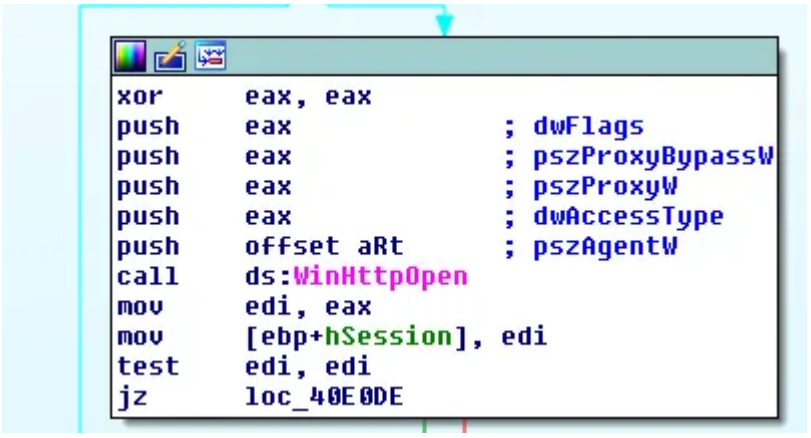
The data gathered is constructed into a JSON blob listing 'Id', 'Domains', 'Group' and 'Server'.

```
push    offset aId      ; "Id"
push    dword_46E02C
mov     dword_46E038, eax
call    sub_402D1F
push    dword_46E030
push    offset aDomains ; "Domains"
push    dword_46E02C
call    sub_401690
push    dword_46E034
push    offset aGroup   ; "Group"
push    dword_46E02C
call    sub_401690
push    dword_46E038
push    offset aServer  ; "Server"
push    dword_46E02C
call    sub_401690
call    sub_402F77
mov     dword_46E03C, eax
call    sub_402F77
mov     dword_46E040, eax
call    sub_402F77
push    offset unk_461EE3
mov     dword_46E044, eax
call    CopyString_4028C4
mov     esi, eax
push    esi
push    dword_46E03C
call    sub_401C9E
push    esi
push    dword_46E040
call    sub_401C9E
push    esi
push    dword_46E044
call    sub_401C9E
push    0
call    j_NetJoinedStatus_40E3FF
pop     ecx
call    j_GetListOfDomains_40E313
call    j_EnumServersInDomain_40E4E0
```

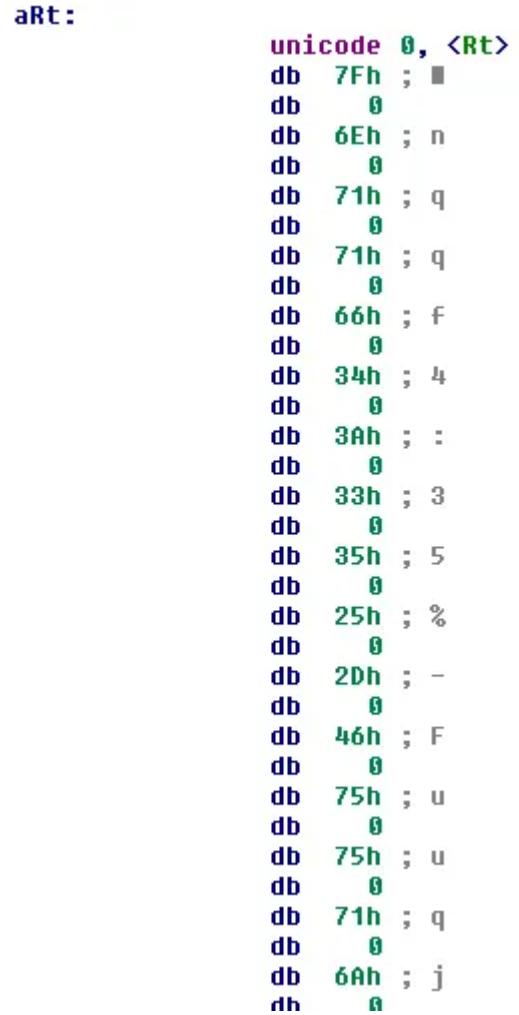
Below is the table explaining what data is harvested:

Name	Data
Id	SHA256 of ComputerName, HwProfileName, HwProfileGuid, CPUID
Domains	Retrieves the DnsDomainName, NetbiosDomainName using DsEnumerateDomainTrusts
Group	GroupStatus and JoinType from NetGetJoinInformation
Servers	Visible servers from domain using NetServerEnum

After all the data has been collected it will simply post it off to the C2, in doing so a hardcoded User-Agent is passed in.



The User-Agent ends up being pretty weird looking but as it turns out the Buer sample that delivered this file had the same User-Agent.

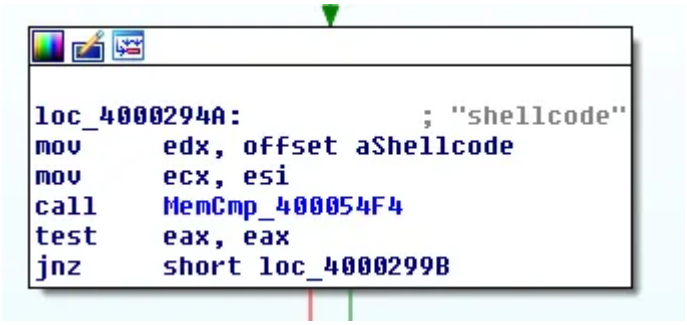


Traffic example:

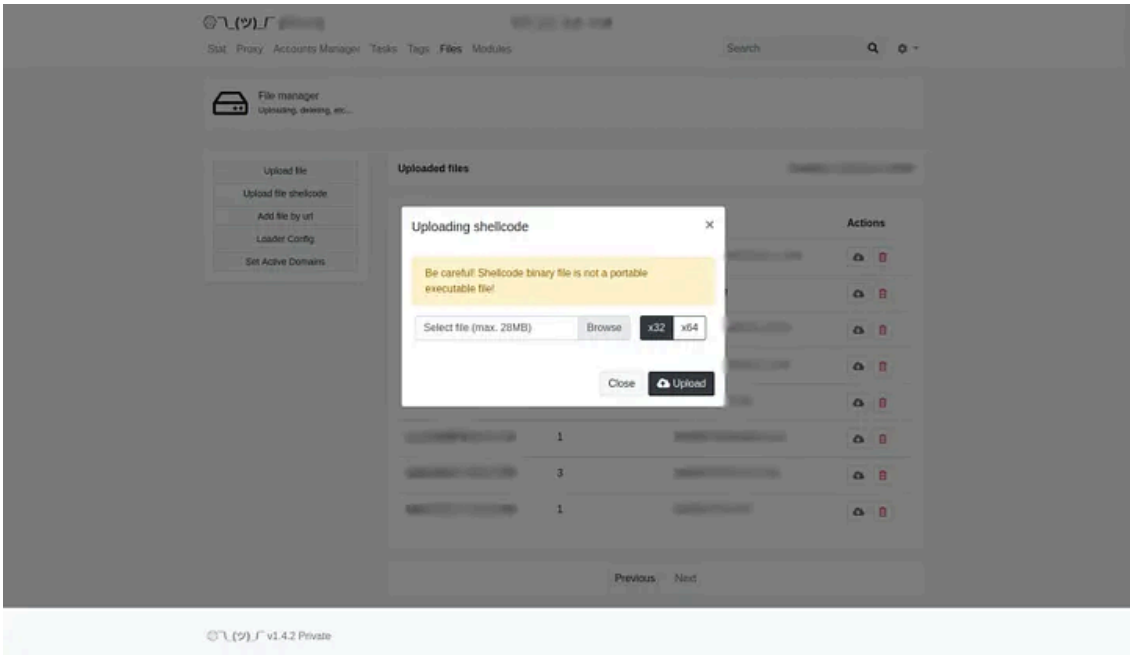
```
POST: /api/v1/modules/domains/dns
User-Agent: Rt\x7fnqqf4:35%-Fuuqj2nUmtsj<H74675739;;@%Z@%HUZ%qnpj%Rfh%TX%]@%js.%Fuuqj\\jgPny49750%-Pl
 "Id": "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855"
 "Domains": {
  "DomainsError": "",
  "DomainsNetBios": [""],
  "DomainsDns": [""]
 },
 "Group": {
  "JoinStatus": "NetSetupWorkgroupName",
  "GroupType": "WORKGROUP"
 },
 "Server": {
  "PCNames": [""]
 }
}
```

ShellCode

Shellcode as a task in Buer has been around but its addition in a bot being leveraged for primarily distributing CobaltStrike makes complete sense as removing a middle man separate stager and allowing Buer to directly load stager shellcode or even a reflectively loaded beacon directly.



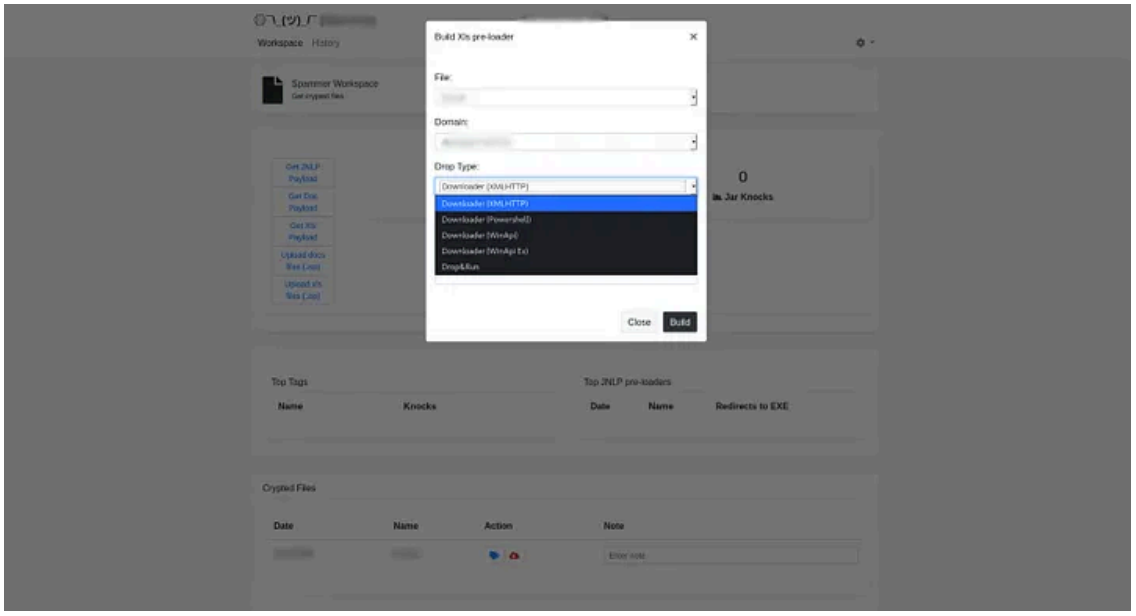
Press enter or click to view image in full size



Spammer Workplace

Buer now also includes the ability to help with spamming through the creation of document based loaders and various delivery chains from the panel:

Press enter or click to view image in full size



Inside the spammer workshop binaries can also be leveraged such as the recently mentioned Rust based loader version from ProofPoint[6]. Buer loader has been one of the most actively developed and updated loaders that we have tracked in 2021.

IOCs

C2s:

```
itmanagersupporter[.]click
hxxps://officewestunionbank[.]com/api/v1/modules/domains/dns
hxxps://tokacpebanking[.]com/api/v1/modules/domain/dns
hxxps://webgraitupeople[.]com/api/v1/modules/domain/dns
```

DomainInfo hashes:

```
38a41e8128ae3955d541c8a00a93de1cd10a01c58368c8254a35659f8627ba30
```

Related OSINT campaigns:

```
https://pastebin.com/U2kNQ3kd
```

References

1:https://www.proofpoint.com/us/threat-insight/post/buer-new-loader-emerges-underground-marketplace

2:https://news.sophos.com/en-us/2020/10/28/hacks-for-sale-inside-the-buer-loader-malware-as-a-service/

3:https://medium.com/walmartglobaltech/cobaltstrike-stager-utilizing-floating-point-math-9bc13f9b9718

4:https://twitter.com/vk_intel/status/1262618254251614215?lang=en

5:https://twitter.com/VK_Intel/status/1359689043735416835?s=20

6:https://www.proofpoint.com/us/blog/threat-insight/new-variant-buer-loader-written-rust

---