BuerLoader Updates

Jason Reaves May 5, 2021

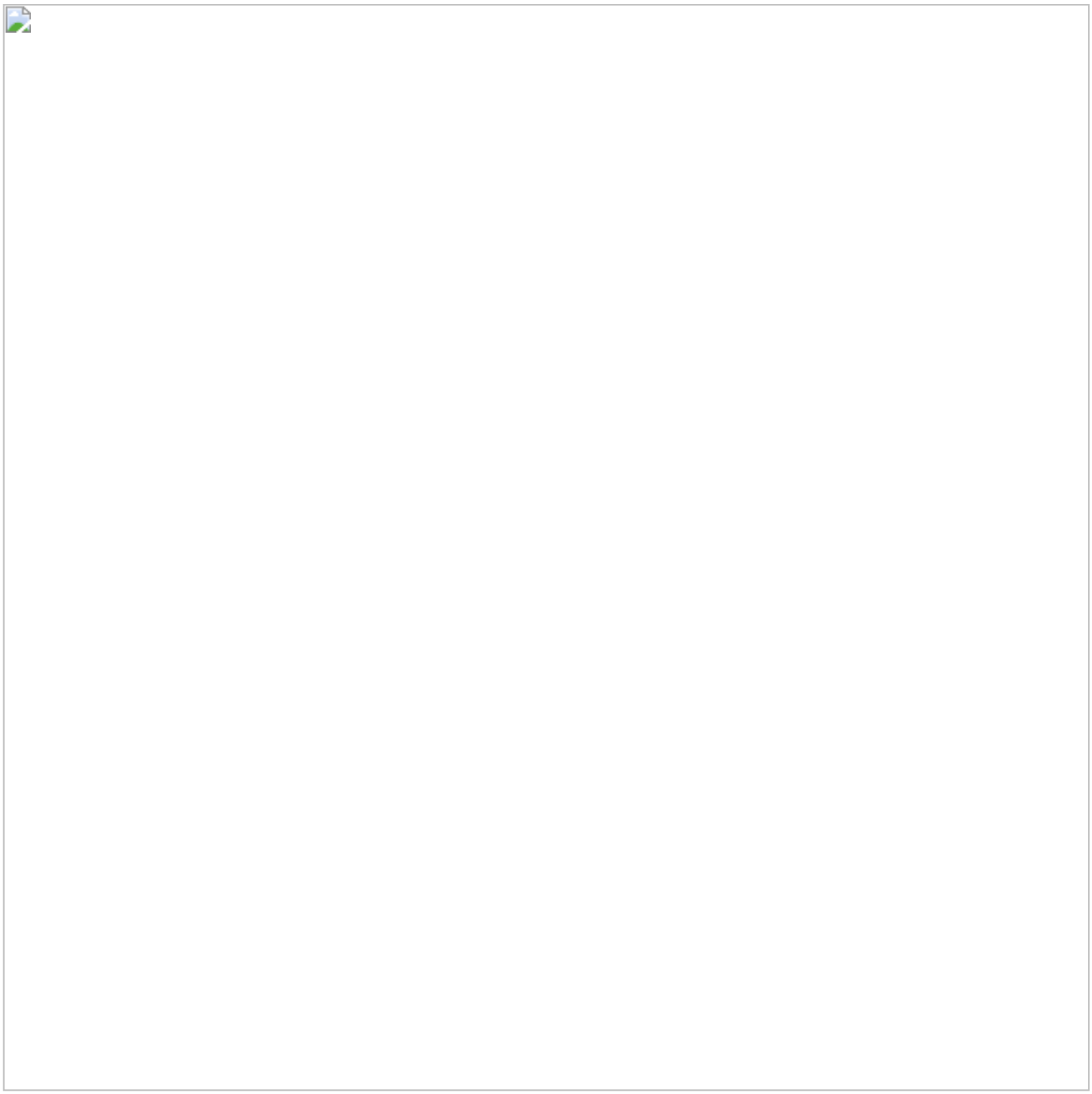
Jason Reaves

May 3, 2021

.

3 min read

By: Joshua Platt and Jason Reaves



Executive Summary

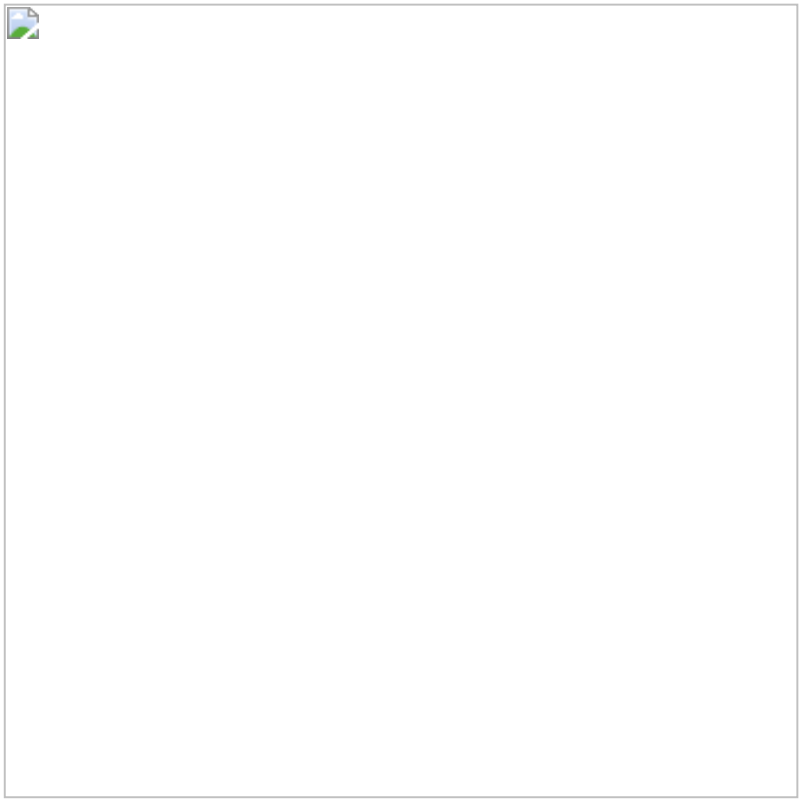
- Buer task includes domain profiler that appears to have code reuse with the version of Buer being leveraged by TrickBots crew
- Buers new functionality around loading shellcode[4] as a task allowing for broader functionality against targets without the need for downloading a separate CobaltStrike stager
- 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.

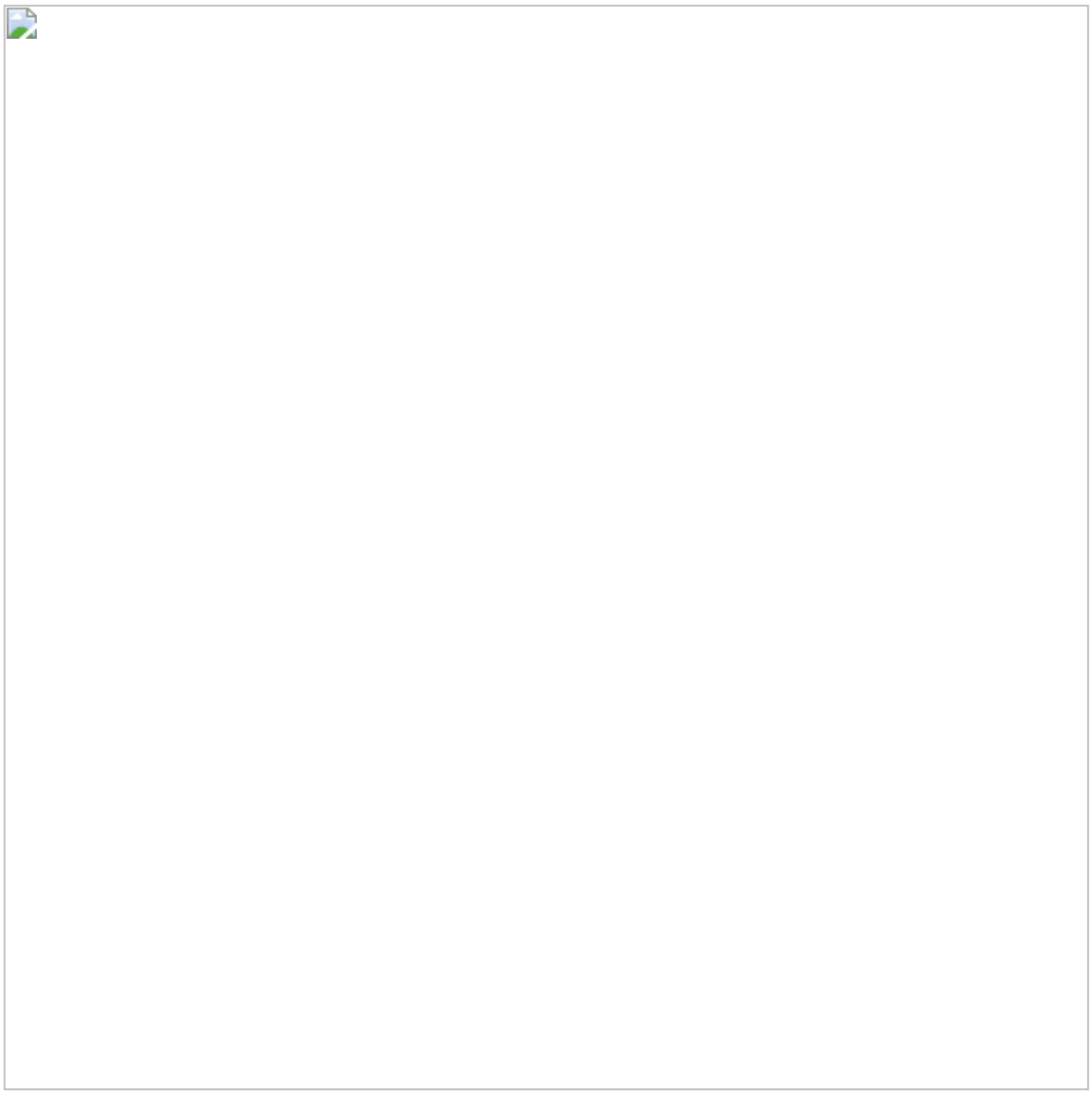
DomainInfo

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

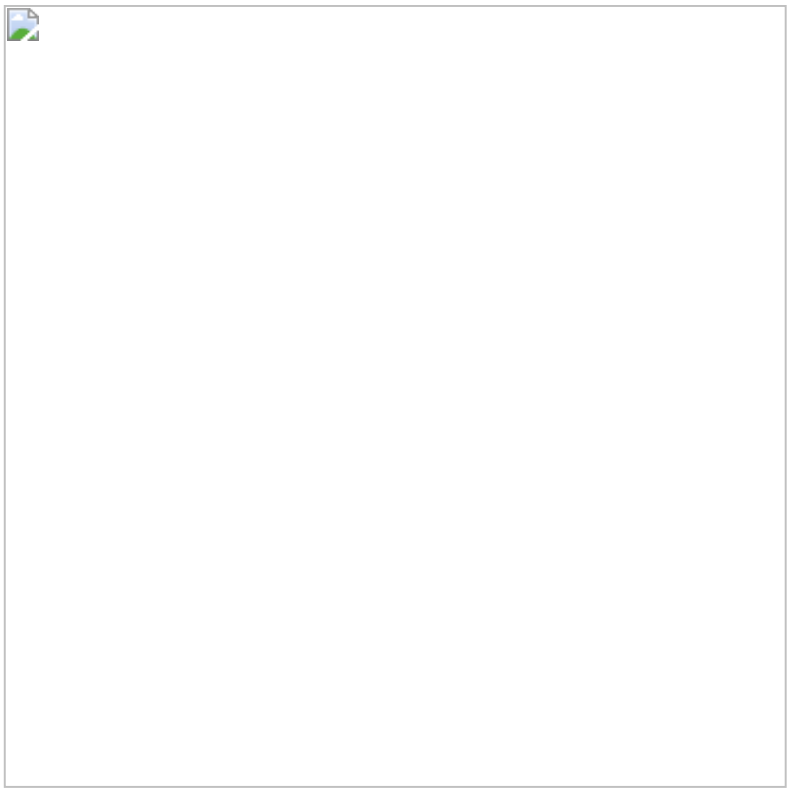
The data gathered is constructed into a JSON blob listing 'Id', 'Domains', 'Group' and 'Server'.



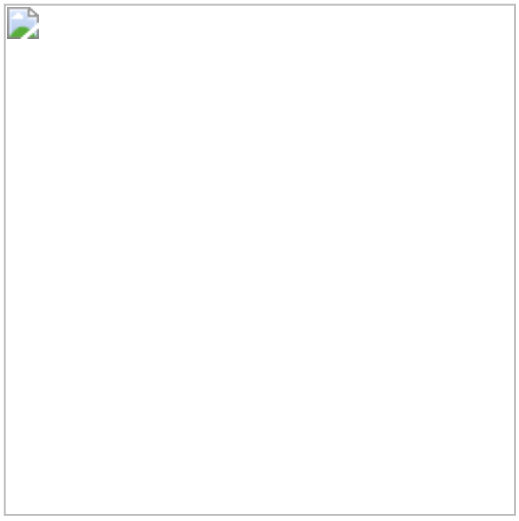
Below is the table explaining what data is harvested:



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.

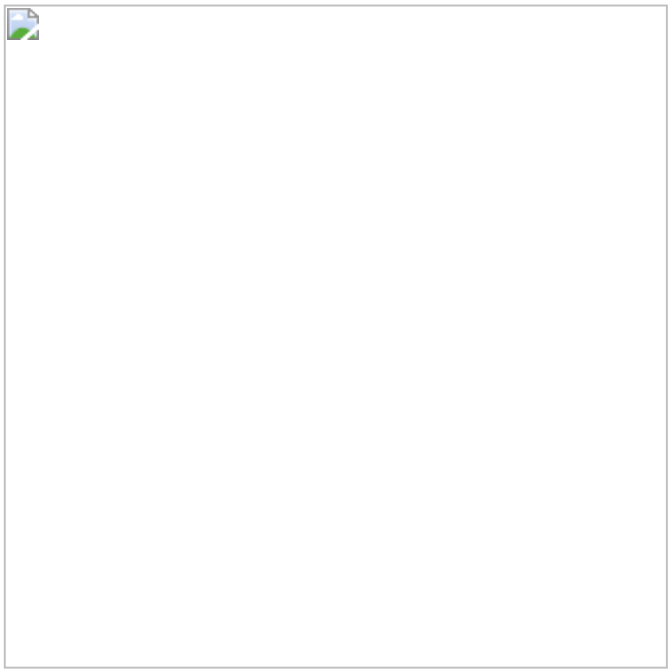


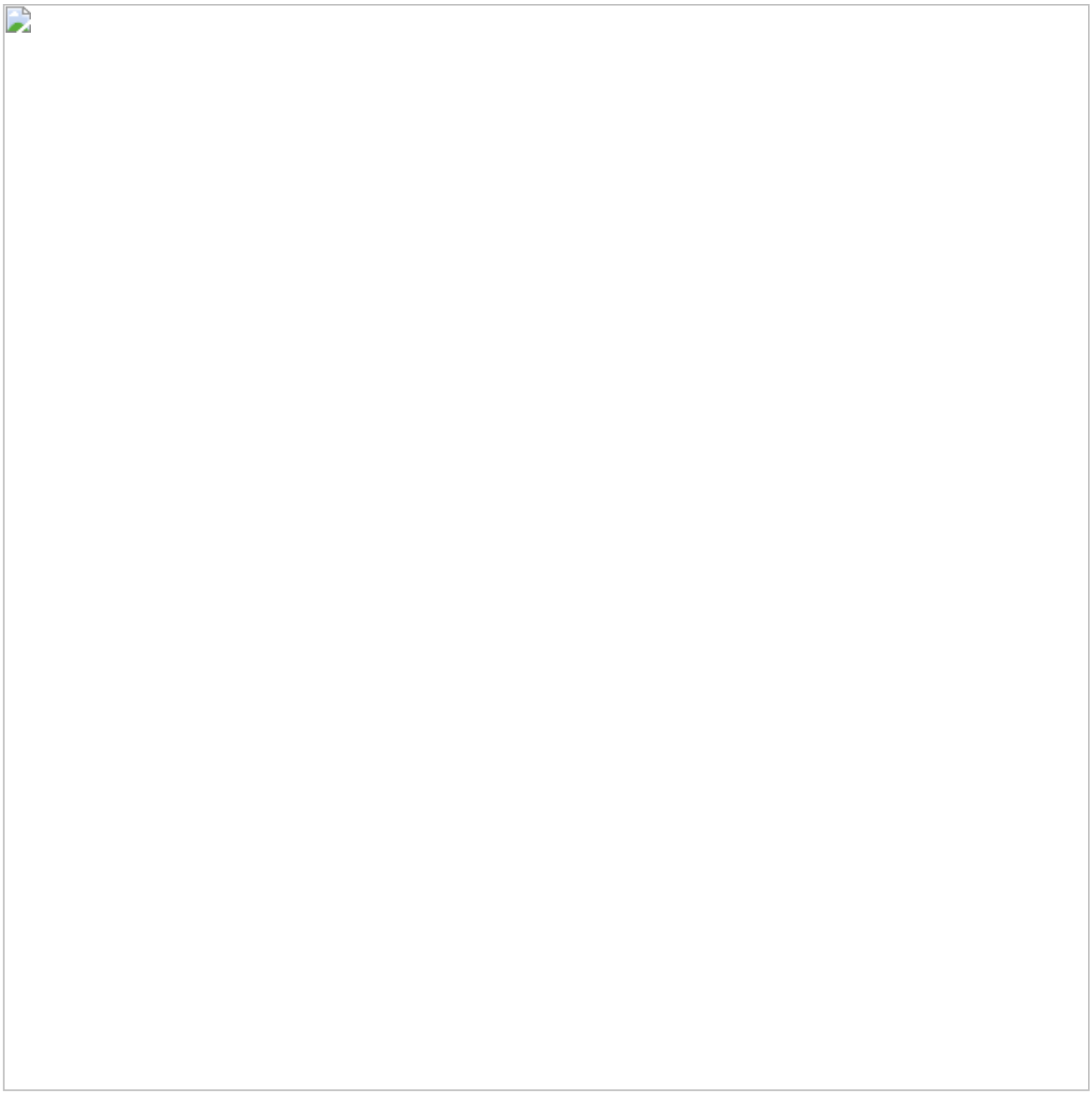
Traffic example:

```
POST: /api/v1/modules/domains/dnsUser-Agent: Rt\x7fnqqf4:35%-
Fuuqj2nUmtsj<H74675739;;@%Z@%HUZ%qnpj%Rfh%TX%]@%js.%Fuuqj\\jgPny49750%-
PMYRQ1%qnpj%Ljhpt.%[jwxnts4835%Rtgnqj46F:98%Xfkfwn496>38{ "Id":
"e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855" "Domains": {
"DomainsError": "",  "DomainsNetBios": [""],  "DomainsDns": [""] }, "Group": {
"JoinStatus": "NetSetupWorkgroupName",  "GroupType": "WORKGROUP" }, "Server": {
"PCNames": [""] }}
```

ShellCode

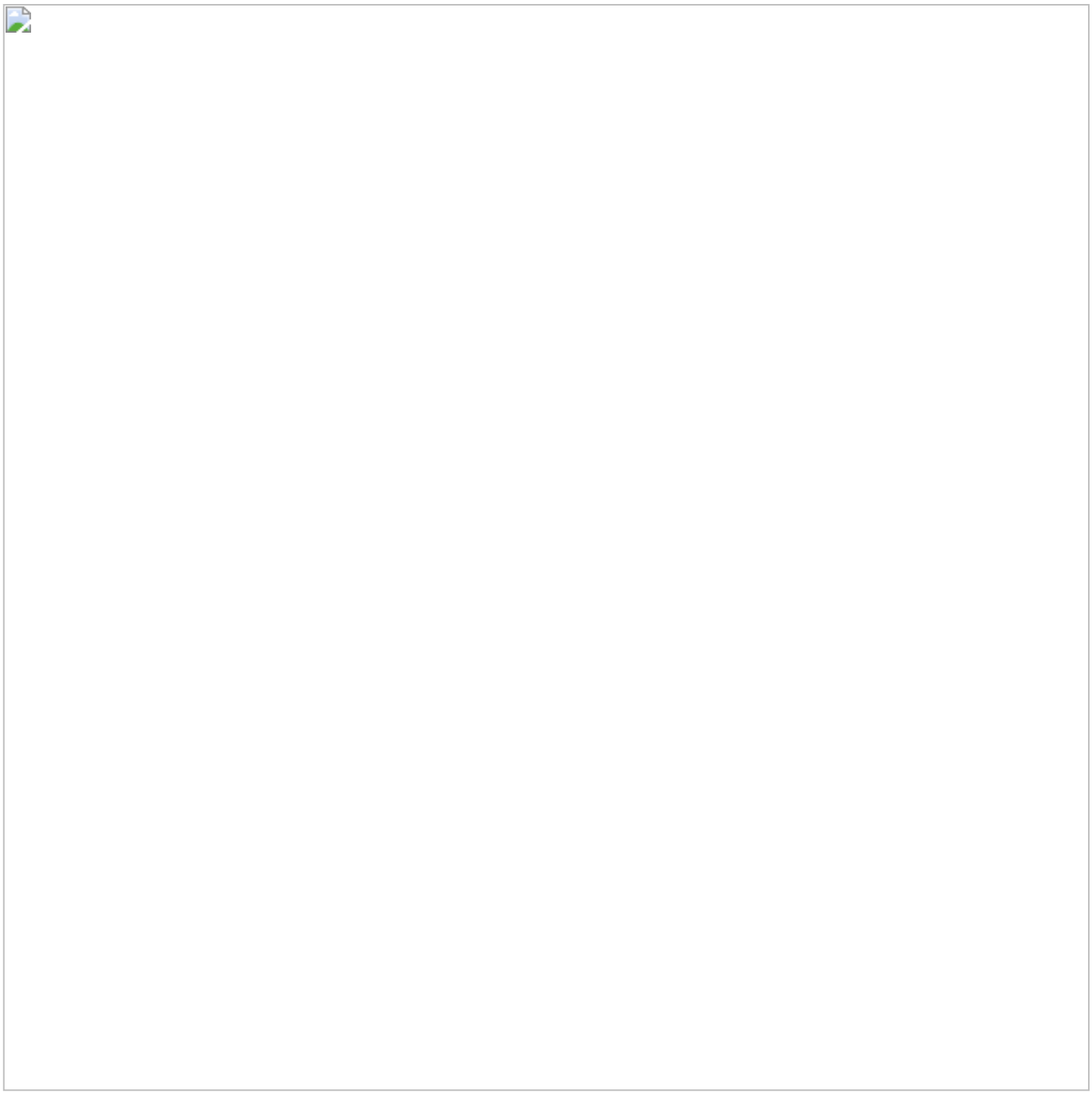
Shellcode as a task in Buer has been around but its addition in a bot being leveraged for primarily distributing CobaltStrike makes complete sense as removing a middle man separate stager and allowing Buer to directly load stager shellcode or even a reflectively loaded beacon directly.





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:



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[.]clickhxxps://officewestunionbank[.]com/api/v1/modules/domains/dnshx
```

DomainInfo hashes:

```
38a41e8128ae3955d541c8a00a93de1cd10a01c58368c8254a35659f8627ba30
```

Related OSINT campaigns:

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