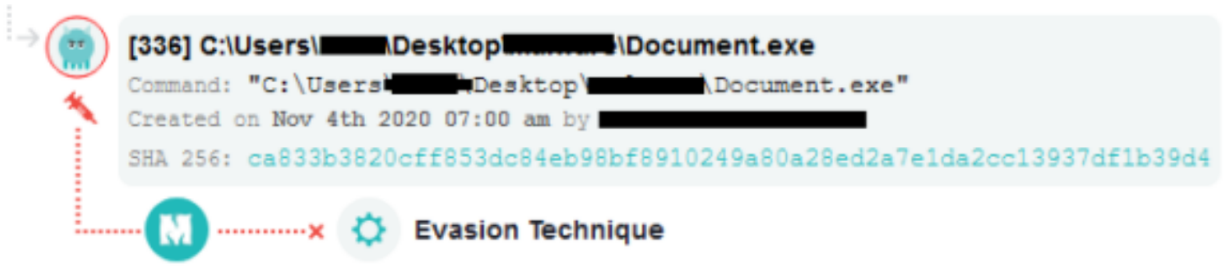
Stopping BuerLoader With Minerva Lab's Hostile Environment Simulation module

blog.minerva-labs.com/stopping-buerloader

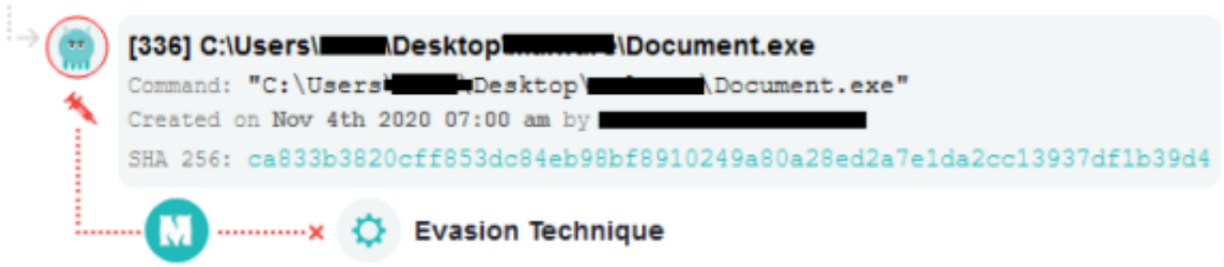


BuerLoader Malware Uses Evasive Techniques To Enter Network Endpoints

Minvera Labs Blocked The Infection

Minerva Labs Blog

News & Reports



BuerLoader Malware Uses Evasive Techniques To Enter Network Endpoints

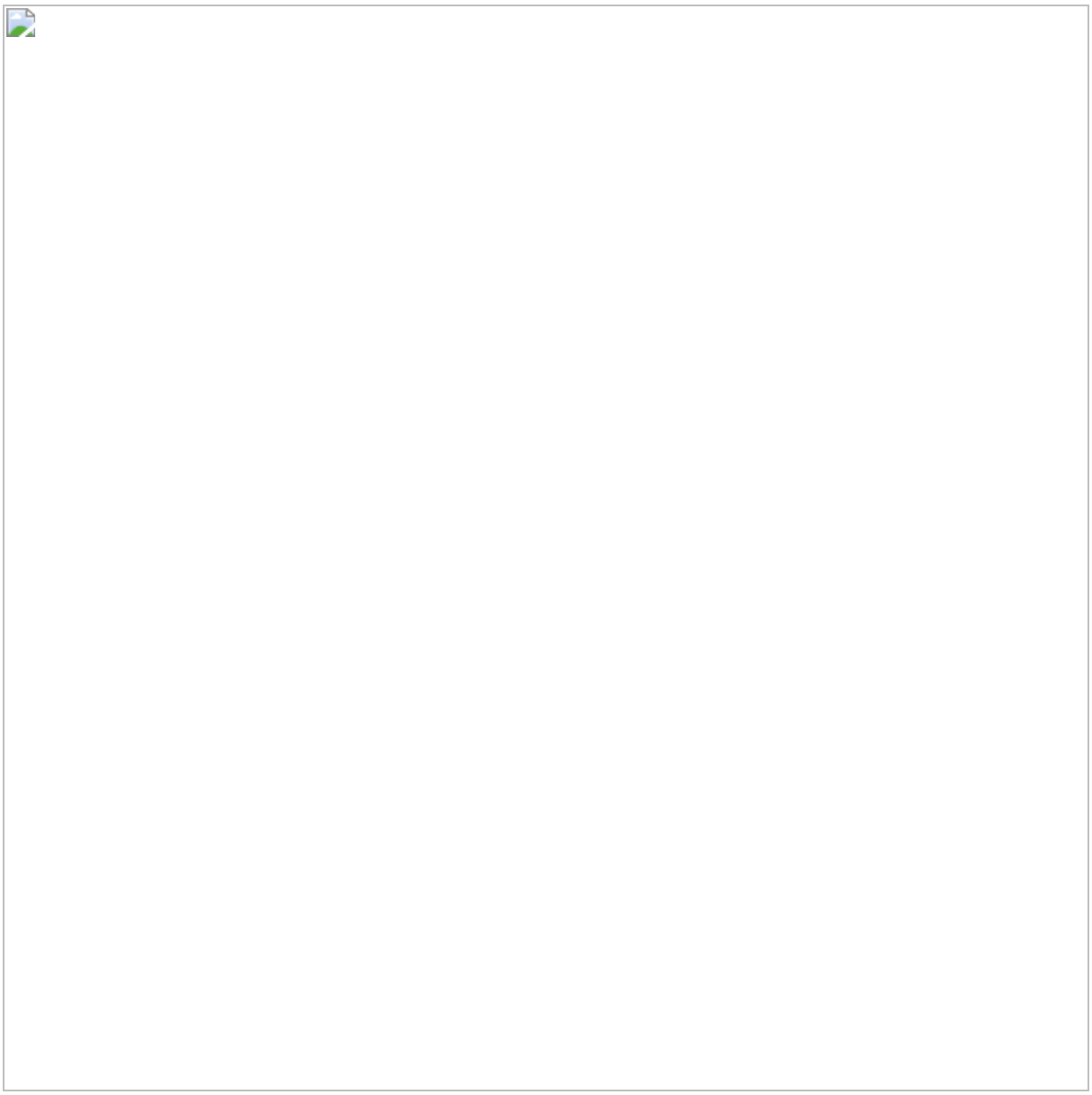
Minvera Labs Blocked The Infection

- Tweet
-

BuerLoader is a stealthy implant, which is frequently used by attackers as an initial foothold in organizations. The malware's common method of infection is by phishing mails, which contain a google docs link with the malicious loader. In our case we have seen the attacker using the invoice payment platform AvidXchange, thus adding another layer of reliability to the mail.

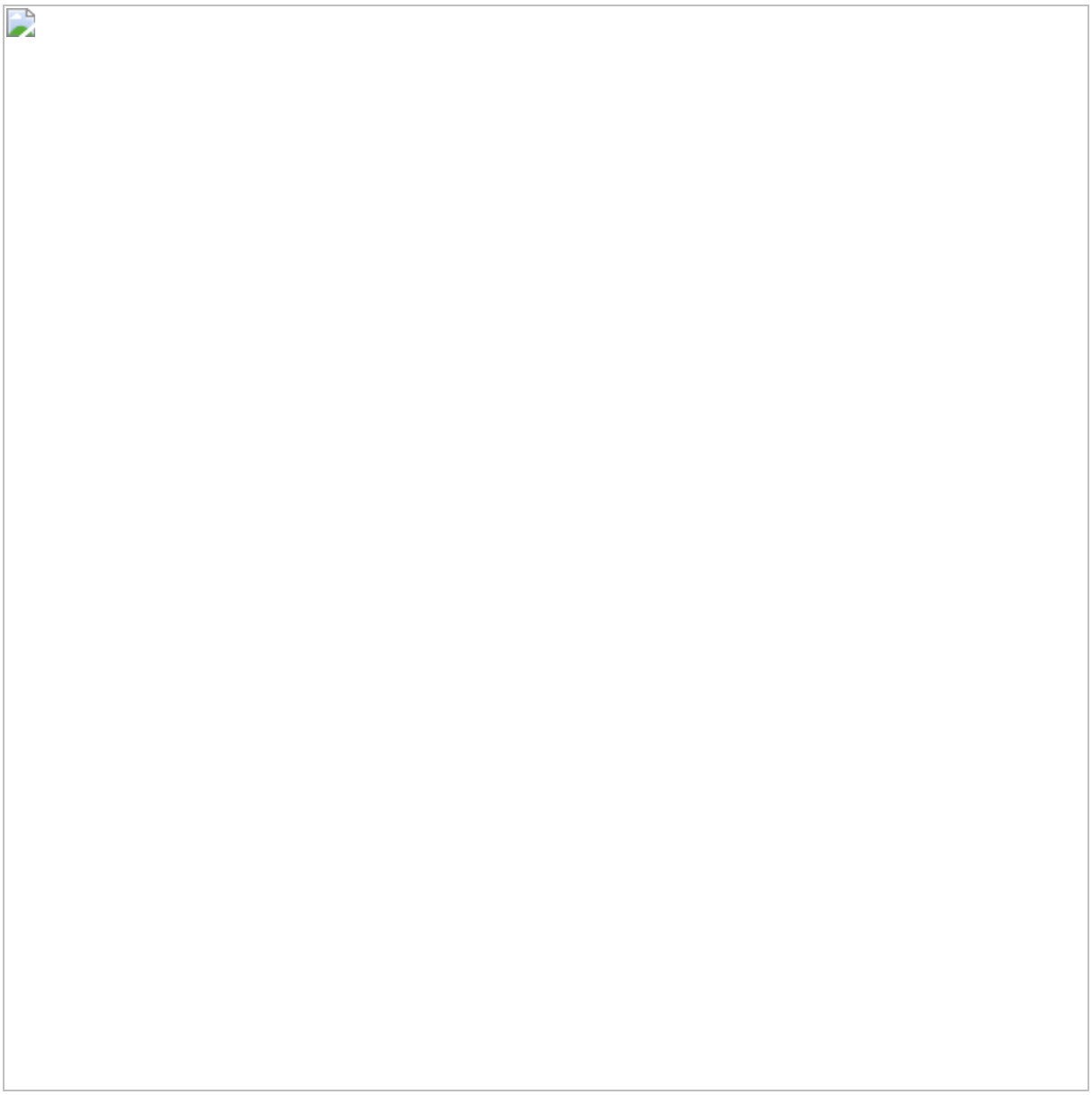
The malware uses a couple of evasive techniques to avoid both sandboxed execution and infecting endpoints in a former Soviet Union state.

First it will use the native function NtQueryDefaultLocale to determine the locale of the machine, and exit if the machine belongs to any of the former CIS countries:



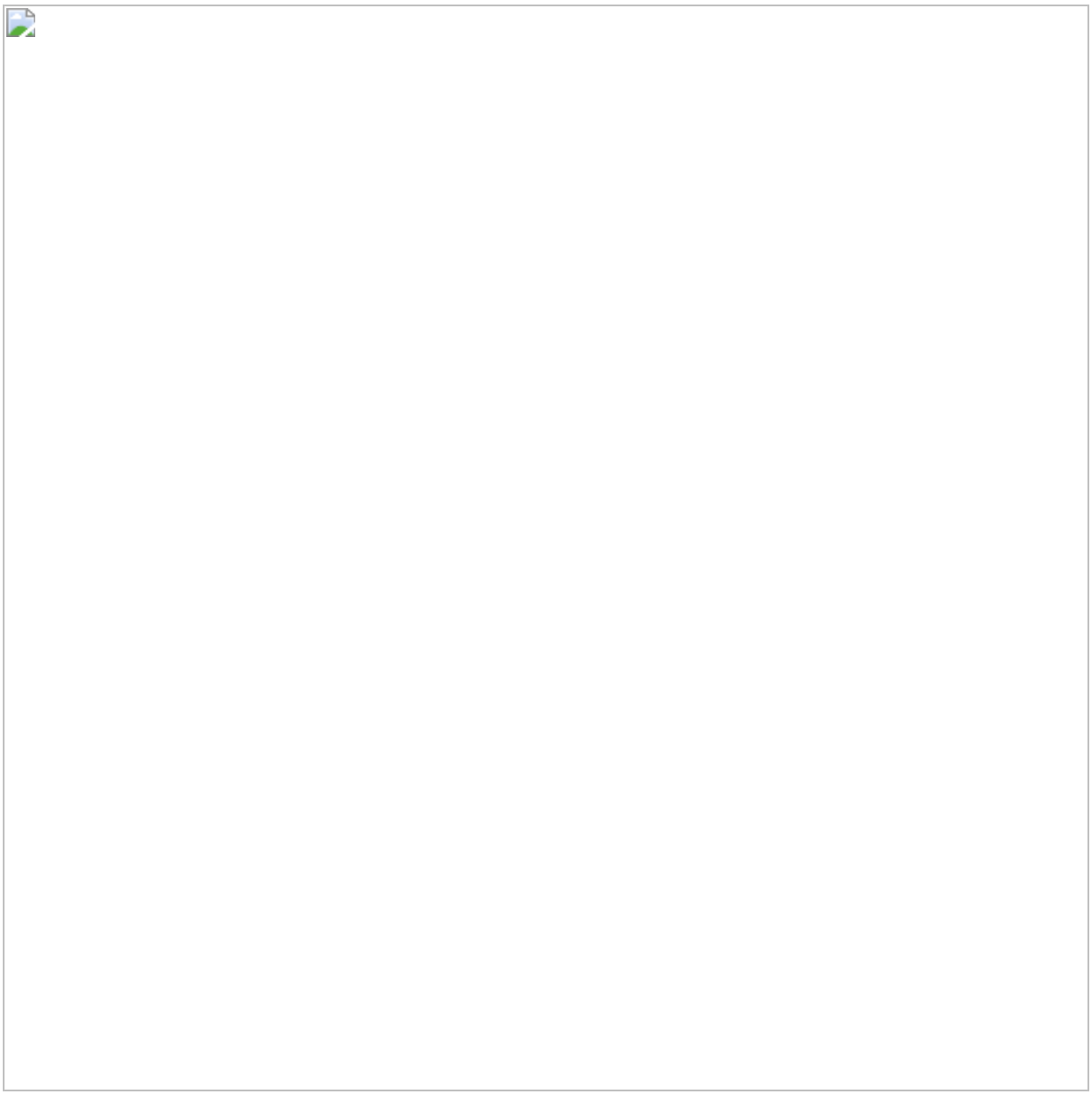
It will then check the size of the machine disk using the windows API function GetDiskFreeSpaceExA, terminating if the total number of free GBs is less than 50 or the total size of the device is less than 120 GBs.

The disk size check in the Buer's code:



Minerva prevents BuerLoader with our Hostile Environment Simulation module, using the malware's code against it.

The event generated by the malware, as seen in Minerva's platform:



IOCs:

Hashes:

ca833b3820cff853dc84eb98bf8910249a80a28ed2a7e1da2cc13937df1b39d4

2b64e34bd7f89d6dbaedebbc59f9e1a905390ad969c40f1696a95feaddbc2295

DNS Names:

https://supsuncorner[.]com/

Mutex:

Uc3nakqfdpmcFjc

« Previous Post
Next Post »

Interested in Minerva? Request a Demo Below