Malspam Campaign Delivers Burkina Trojan

blogs.infoblox.com/cyber-threat-intelligence/cyber-campaign-briefs/malspam-campaign-delivers-burkina-trojan/

Infoblox Cyber Intelligence Group March 29, 2021

Author: Jeremy Ware

TLP: WHITE

Overview

From 21 to 23 March, we observed a malspam campaign distributing the Burkina trojan. First seen in October 2017, Burkina is a trojan distributed through executable (EXE) files sent via email.

Customer Impact

Burkina infects a victim's computer and attempts to harvest credentials, interrupt standard processes, conceal network connections, and other malicious actions. The malware then reaches out to a command and control (C&C) server to receive additional instructions.

The threat actor can use the stolen credentials to carry out additional malicious acts, including dropping a ransomware package or distributing additional payloads such as Trickbot.[1]

Campaign Analysis

The campaign we observed delivered Burkina via spam emails. Both the subject line – *WG:Re:AG:Re:New order.* – and body – *See attached PDF* – of each message were identical. The emails carried a malicious EXE attachment masquerading as a PDF with the filename *SPL6677.pdf.exe*.

Attack Chain

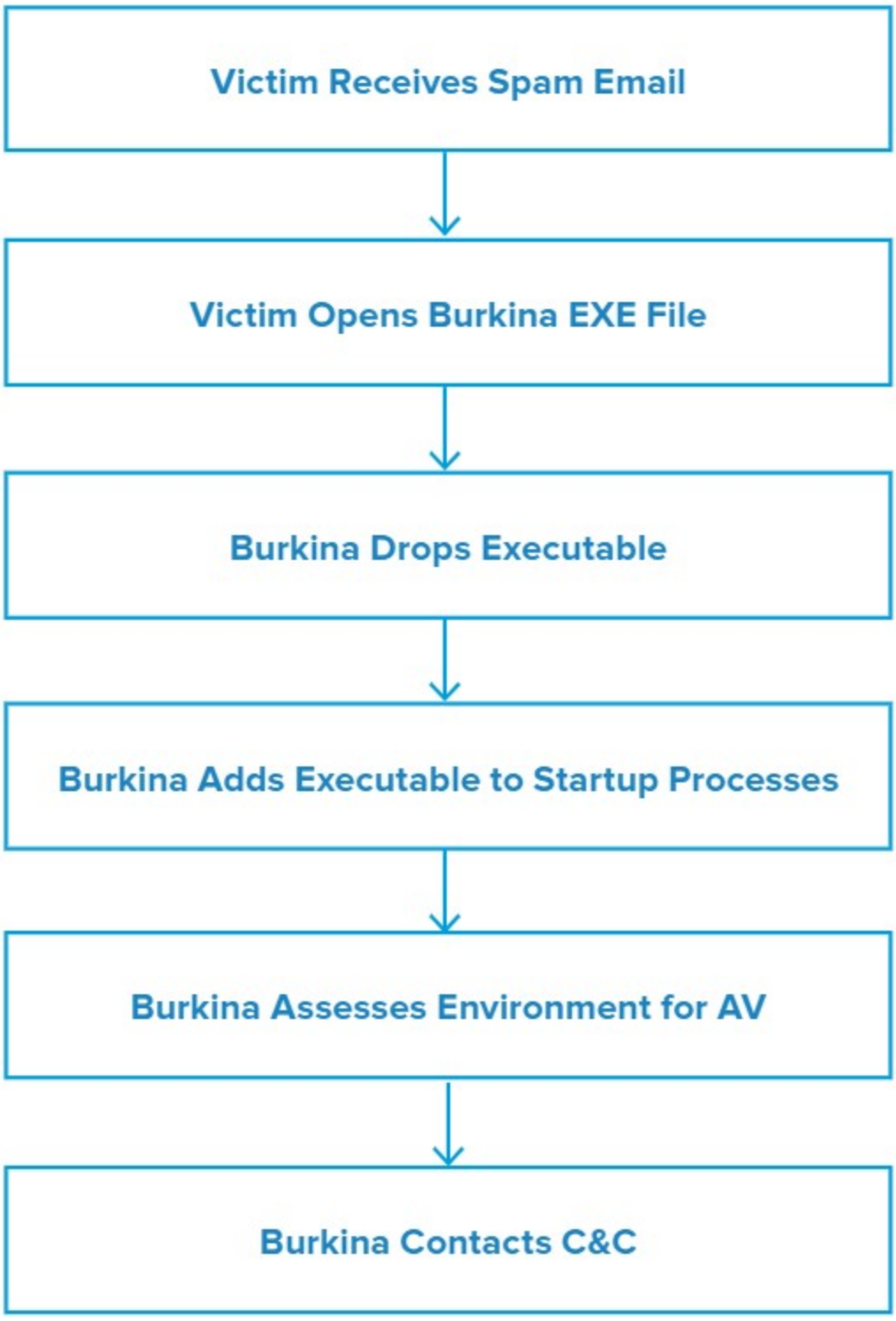
Once the user opens the attached file, the executable will present the message "SimpleGameLib has stopped working" to the user.

Burkina drops another executable file named *WerFault.exe* and updates the AutoRun Registry to include itself. It then attempts to harvest credentials and saved passwords once the user opens a browser. Finally, the malware attempts to connect to a C&C server to receive further instructions as well as to exfiltrate the stolen data.

Vulnerabilities & Mitigation

Infoblox recommends the following precautions to reduce the possibility of infection by Burkina:

- Be cautious of emails from unfamiliar senders and inspect unexpected attachments before opening them.
- Always be suspicious of vague emails, especially if there is a prompt to open an attachment or click on a URL or clickable text.
- Filter attachments to reduce the likelihood of malicious content reaching a user's workstation.
- Be aware of any attachment's file type and never openfiles that could be a script (.vbs, .cmd, .bat) or another executable (.*exe*).
- Ensure you read the file type correctly as many threat actors will include a trusted file type description in the name (.pdf, .docx, .xls, etc.)



Endnotes

1. https://www.joesandbox.com/analysis/325825/0/html/
2. https://howtofix.guide/heur-msil-burkina-1/