Buer Loader Campaign Spoofs Identity Services Company

Author: James Barnett

Overview

From February 2 to 10, Infoblox observed an ongoing malspam campaign delivering trojan malware known as Buer Loader. This campaign used invoice-themed lures to entice users to download and open Microsoft Excel (XLS) documents that contain malicious macros and spoof GlobalSign, a legitimate identity services company.

Customer Impact

Buer Loader is a trojan downloader that is used to compromise a targeted system and deliver additional malicious payloads. It is sold to threat actors using a "malware-as-a-service" payment model and was first identified in August 2019 after the author advertised it on an underground hacking forum.[1]

The methods used to distribute Buer vary between threat actors, but it is commonly distributed via malspam. It has also been observed as a payload delivered by RIG exploit kit.[2,3]

Campaign Analysis

The emails in this campaign used an invoice-themed lure to entice targets into opening an attached XLS document. The subject lines of the emails contained generic invoice numbers. The email bodies contained a randomized invoice template thanking the recipient for their business, listing charges for arbitrary products, and prompting the recipient to view the attached file for additional information about their alleged order. These attachments contained graphics and text that mimic the legitimate company GlobalSign.

Attack Chain

When the victim opens the attached XLS document, Excel displays a warning that a circular reference in the spreadsheet may cause the formulas in it to behave incorrectly. This warning prevents the document's malicious macros from executing until the victim manually dismisses it. While it is not clear whether the threat actor intended for the spreadsheet to generate this error, it may serve to ensure that the document is opened by a real person rather than an automated malware analysis platform.

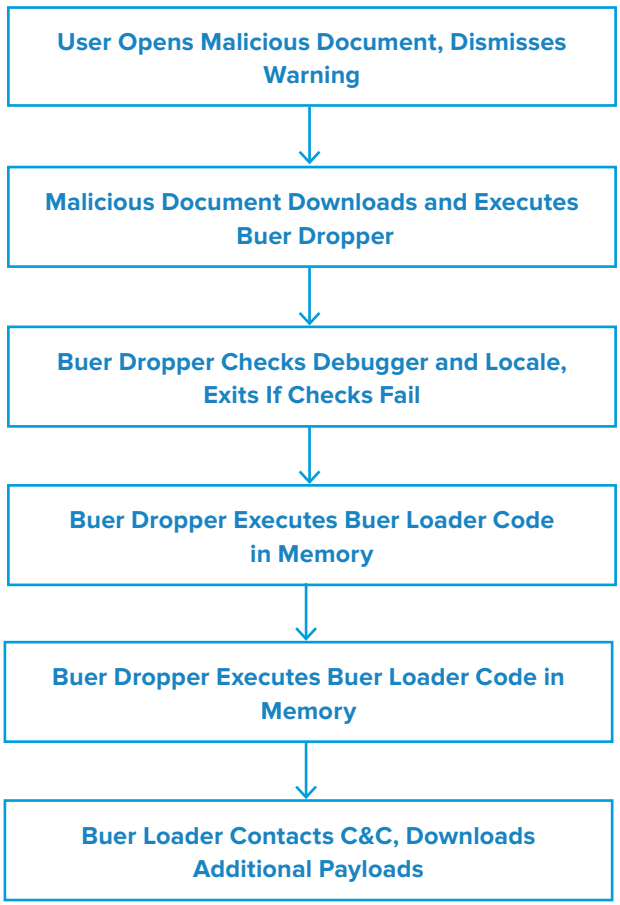
When the user dismisses the warning, the malicious macros in the document download and execute the initial Buer dropper payload from a remote location. This dropper checks for the presence of debuggers commonly used for forensic malware analysis and halts execution if it finds any.

If the dropper does not find debuggers, it checks the system's language and localization settings to infer the geographic location of the victim's system. The dropper will immediately halt execution if the settings appear to match a country in the Commonwealth of Independent States (CIS), a group of countries that were formerly part of the Soviet Union. This is a common behavior exhibited by malware developed in CIS countries.

If the system passes the dropper's checks, the dropper unpacks the primary Buer Loader payload and executes it directly in memory. Because this process does not produce an additional payload file for the main Buer payload, the infection is more difficult to detect and remove than a more traditional file-based malware infection.

Once the Buer Loader payload is running in memory, it executes two PowerShell commands. The first command allows Buer to bypass PowerShell execution warnings to ensure the victim will not be alerted to any future PowerShell commands it attempts to execute. The second command adds exceptions to Windows Defender to prevent it from scanning Buer's additional payloads when the loader downloads them.

After executing these two PowerShell commands to improve its evasiveness, Buer Loader reads the system GUID from the Windows Registry and communicates the information to its command and control (C&C) to identify itself as a newly-compromised system. The malware continues to communicate with this C&C to receive further instructions from the threat actor. These instructions generally involve downloading and executing additional malware payloads, but the samples we analyzed did not deliver any additional payloads during our analysis.



Vulnerabilities & Mitigation

Infoblox recommends the following actions to reduce the risk of this type of infection:

- Be cautious of emails from unfamiliar senders and inspect unexpected attachments before opening them.
- Always be suspicious of vague or empty emails, especially if there is a prompt to open an attachment or click on a link.
- Implement attachment filtering to reduce the likelihood of malicious content reaching a user's workstation.
- Do not open attachments that are unexpected or from unfamiliar senders.
- Never enable macros, and do not configure Microsoft Office to enable macros by default. Macros are a very common infection vector used by many families of malware.

Endnotes

1. https://news.sophos.com/en-us/2020/10/28/hacks-for-sale-inside-the-buer-loader-malware-as-a-service/
2. https://www.malware-traffic-analysis.net/2021/02/04/index.html
3. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--50