LokiBot Campaign Uses Microsoft Office Exploit

Author: Darby Wise

Overview

On December 9, Infoblox observed a malicious email campaign exploiting CVE 2017-11882[1] to distribute LokiBot malware. This campaign used purchase order-themed lures to entice victims into downloading malicious Microsoft Excel (XLS) files.

We have previously written several reports on LokiBot, including campaigns that used Coronavirus-themed lures, NGROK tunneling to download payloads, and malicious RTF files to infect victims.[2,3,4]

CVE 2017-11882, a stack buffer overflow vulnerability in the Microsoft Equation Editor, is an exploit commonly used by threat actors. This past week, we observed a number of similar campaigns that use this CVE in their attack chains and distribute malware such as Agent Tesla, Formbook and AveMaria.

Customer Impact

LokiBot is a popular information stealing trojan first observed in 2015 and is frequently distributed through malspam campaigns. It is capable of harvesting the victim's login credentials, cryptocurrency wallets and other sensitive information through various methods such as keylogging. The malware then reports the stolen information to a command and control (C&C) server.[5]

LokiBot is also capable of establishing backdoors that enable the attacker to install additional payloads.

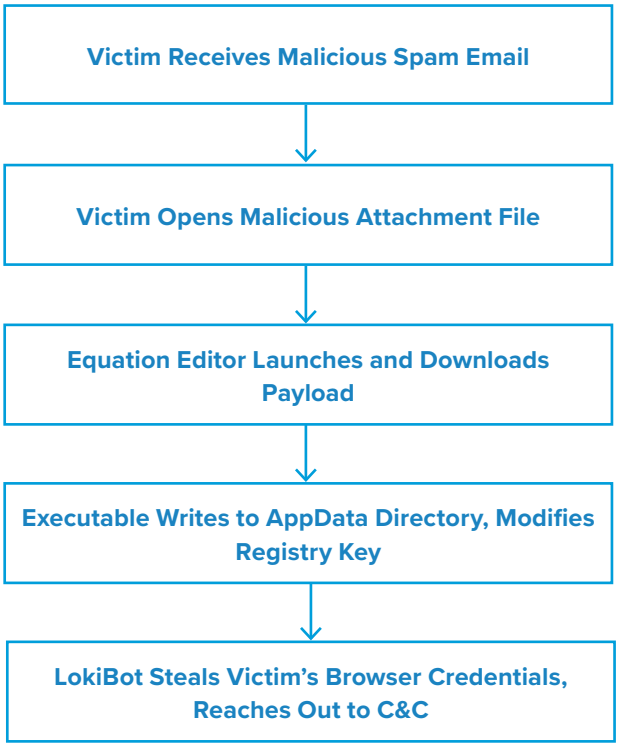
Campaign Analysis

Threat actors used a common malspam theme referencing purchase orders in this campaign. Email subjects included *Purchase Order Confirmation for December 1st Lot and ORDER CONFIRMATION*. All of the emails contained an attached XLS file named Purchase Order Confirmation.xlsx. The email bodies were either empty or contained a short greeting such as "Dear All" and "Good day."

Attack Chain

When the victim opens the XLS file attachment, it automatically exploits CVE 2017-11882 to download and run the LokiBot payload (*vbc.exe*).

To maintain persistence, the executable writes itself into the user's AppData directory and modifies a registry key. Finally, the malware begins to steal the victim's browser credentials, along with other personal data, and transmits it to its C&C server.



Vulnerabilities & Mitigation

Malicious spam attachments are the primary infection vector for LokiBot. Infoblox recommends the following actions to reduce the risk of this type of infection.

- Always be suspicious of unexpected and vague emails and unknown senders.
- Do not open attachments that are unexpected or from unfamiliar senders.
- Exercise additional caution when unexpected messages or attachments have commonly used themes such as shipping or financial documents or advice.
- Verify important or potentially legitimate attachments with the sender via alternative means such as a phone call or separate email to a known contact.

Endnotes

1. https://nvd.nist.gov/vuln/detail/CVE-2017-11882
2. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--62
3. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--16
4. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--27
5. https://us-cert.cisa.gov/ncas/alerts/aa20-266a