Formbook Information Stealer

Author: James Barnett

Overview

On 2 January, Infoblox observed an email campaign that used malicious ZIP attachments to distribute Formbook malware.

Formbook is ready-made malware that can be purchased and deployed by any threat actor.[1] It is primarily distributed through email campaigns that entice victims to open a malicious attachment. The nature of the attachment varies depending on the threat actor distributing it, but Formbook is packaged as a self-extracting RAR archive by default.[2]

Customer Impact

Formbook is an information stealer that uses form grabbing techniques to harvest login credentials and other sensitive data from web forms. Form grabbing is similar to keylogging in purpose, but with the advantage that it can also capture data that has been autofilled or pasted into a web form in addition to data that is typed.

Campaign Analysis

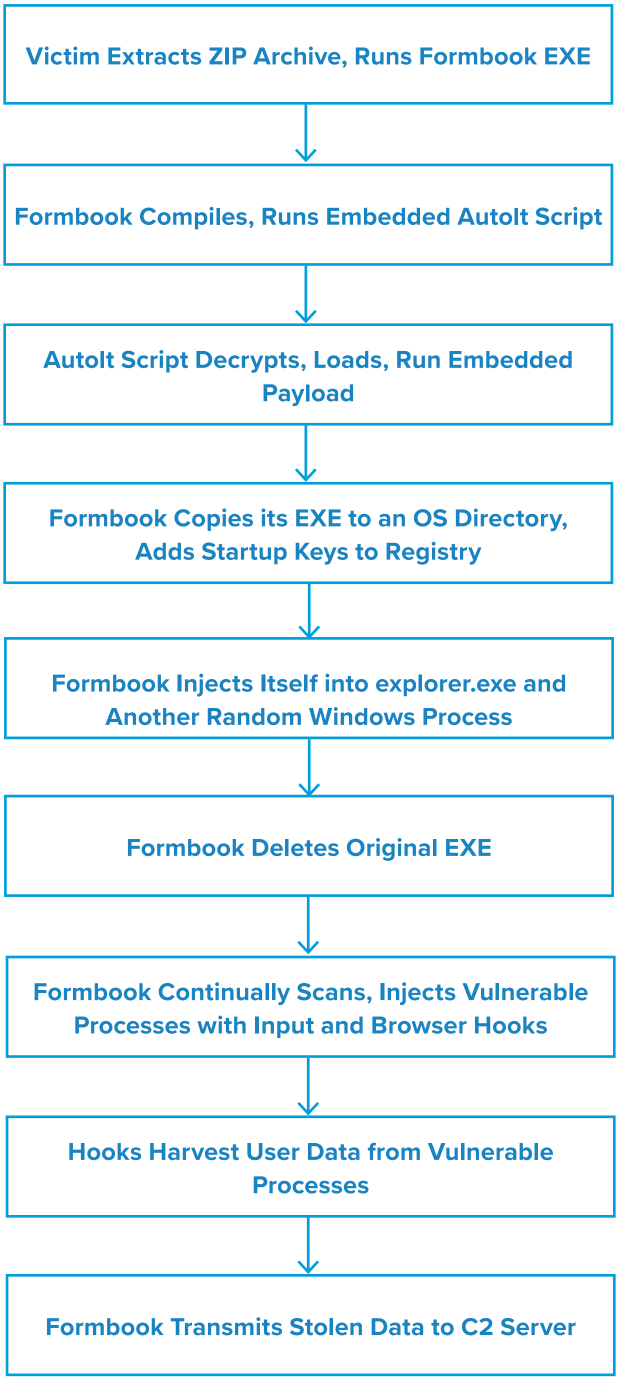
The Formbook campaign that Infoblox observed used an invoice payment theme to entice victims to open a Formbook executable file contained within a ZIP archive. The body text of these emails requested that the recipient confirm the details of a pending invoice to receive payment. The email attachments played into this theme by using deceptive filenames and icons to give the impression that they were PDF documents.

Attack Chain

When the victim runs the Formbook executable contained within the ZIP file, it starts to compile and execute an embedded AutoIt script. This script decrypts an embedded Formbook payload, loads it into memory, and executes it.

Upon execution, the Formbook payload copies itself to a randomly-named directory within one of several Windows operating system (OS) directories. Formbook selects the directory based on the privileges it has when it runs. When Formbook has elevated privileges it copies itself to the "Program Files" directory. When Formbook has standard privileges it copies itself to the current user's profile folder, the user-specific "AppData" directory, or the Windows "Temp" directory.

After copying itself to a new location, Formbook continues to establish its persistence by creating registry entries that tell Windows to run the new Formbook executable on startup. It also uses the CRC32 checksum of explorer.exe to locate the Windows Explorer process. Formbook then injects itself into the Windows Explorer process as well as another randomly-chosen operating system process. If this process injection is successful then Formbook proceeds to delete the executable that was initially used to install it.


Victim Extracts ZIP Archive, Runs Formbook EXE
Formbook Compiles, Runs Embedded AutoIt Script
AutoIt Script Decrypts, Loads, Run Embedded Payload
Formbook Copies its EXE to an OS Directory, Adds Startup Keys to Registry
Formbook Injects Itself into explorer.exe and Another Random Windows Process
Formbook Deletes Original EXE
Formbook Continually Scans, Injects Vulnerable Processes with Input and Browser Hooks
Hooks Harvest User Data from Vulnerable Processes
Formbook Transmits Stolen Data to C2 Server

Once Formbook infects the system it enters a loop that scans the list of current processes for programs it can attack. Formbook's list of targets includes every popular web browser (e.g. Chrome, Firefox, Internet Explorer, and Microsoft Edge) as well as several less common ones. Formbook can also target email clients such as Microsoft Outlook and Thunderbird, as well as file browsers including Windows Explorer and Total Commander.

When Formbook identifies that a vulnerable process is running, it injects itself into that process to monitor its activity. It uses a suite of keyboard and clipboard hooks to intercept user inputs, plus a set of browser hooks that can scan HTTP requests for potential user credentials. It then transmits this stolen data to a command and control (C2) server controlled by the attacker.

Vulnerabilities & Mitigation

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

- 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.
- Be aware of any attachment's file type, and never open files that could be a script (.vbs, .cmd, .bat), an internet shortcut file or compression file. Using the latter is a known method for evading detection methods based on file hashes and signatures. Threat actors use them to mask the real malicious file due to email service restrictions on attachment file types.

Endnotes

1. https://thisissecurity.stormshield.com/2018/03/29/in-depth-formbook-malware-analysis-obfuscation-and- process- injection/
2. https://www.fireeye.com/blog/threat-research/2017/10/formbook-malware-distribution-campaigns.html

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com