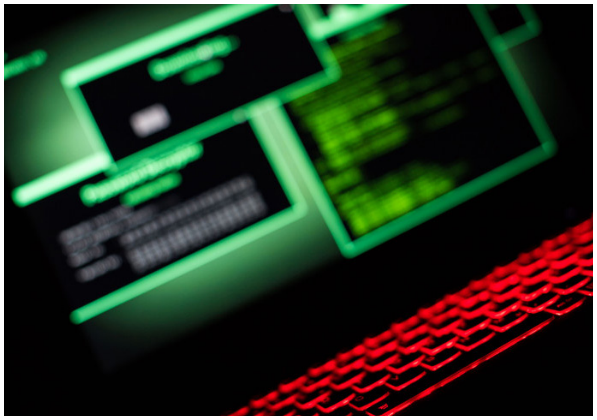
Infoblox
NEXT LEVEL NETWORKING

Linked SWIFT-Themed Campaigns Deliver Keyloggers and Infostealers



Overview

From 1 through 6 February, we observed several campaigns using malicious spam emails (malspam) with themes pertaining to SWIFT payments or SWIFT copies.[1] Using financial-themed lures is a common tactic for designing malspam, and SWIFT documents are regularly referenced in subject lines and attachment file names.

The malspam campaigns we found delivered several malware families, including Agent Tesla keylogger, Lokibot infostealer, Hawkeye keylogger, and Formbook infostealer. The tactics, techniques, and procedures appear similar to activity conducted by the threat actor SWEED, as reported by Talos in July 2019.[2]

Customer Impact

We have written about previous malspam campaigns delivering all of the above-mentioned malware. Agent Tesla, the predominant malware in the February campaigns, can capture and store keystrokes, steal credentials, and exfiltrate data to a command and control (C2) server, potentially via email messages to a remote mail server. Lokibot harvests victim credentials and reports them to an attacker-controlled C2 server.

Hawkeye can log keystrokes and clipboard data, and steal credentials from email and web applications. Formbook's capabilities include process hollowing, clipboard monitoring, keylogging, webform hijacking, and downloading additional payloads.

Campaign Analysis

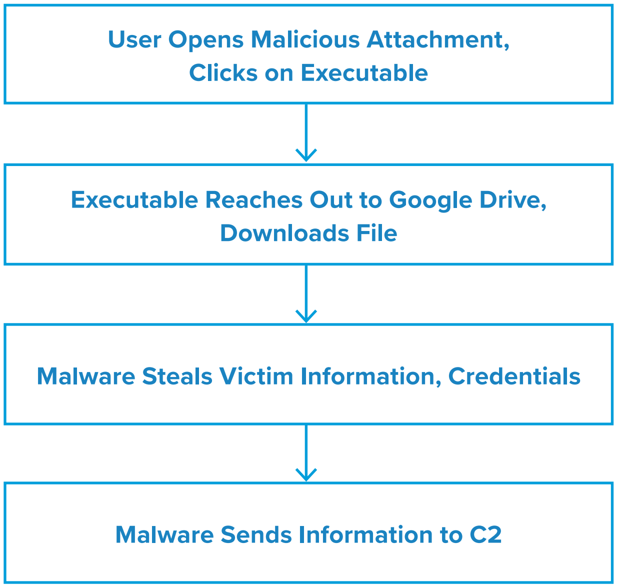
All of the emails we discovered used the acronym “SWIFT” either in the subject line or the attachment's file name. Many of the messages alleged to contain an outstanding invoice, or spoofed correspondence from popular banks such as Standard Charter and Wells Fargo.

Beyond that, the messages varied significantly. Some had content in the message body, while others were empty. Most of the files were compressed and included the following types: ZIP, RAR,[3] GZ,[4] ISO,[5] and LZH.[6]

At this time, we have not identified targeted groups for these campaigns; however, there was a small percentage of messages that referred to a bank in Romania, or had URLs with German or Russian cTLDs. The URL with the Russian cTLD was malicious.

Attack Chain

The attack chains varied somewhat across the campaigns, but all required the recipient to open an attached file that was often compressed. Many of the samples reached out to Google Drives and downloaded files that matched the following pattern: [a-zA-Z]{3,}_encrypted_[0-9A-Z]{7}\[1\].bin.



User Opens Malicious Attachment, Clicks on Executable

Executable Reaches Out to Google Drive, Downloads File

Malware Steals Victim Information, Credentials

Malware Sends Information to C2

Vulnerabilities & Mitigation

The threat actor used malicious spam emails to distribute all of the malware for this campaign. As such, we recommend the following actions to reduce the risk of this type of infection:

- Regularly train users to be aware of potential phishing efforts and how to handle them properly.
- Always be suspicious of unexpected and vague emails and unknown senders.
- Do not open files attached to emails that are suspicious or from unknown 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.
- Check order statuses by browsing directly to the delivery website, rather than using an embedded link.

Endnotes

1. SWIFT stands for Society for Worldwide Interbank Financial Telecommunication. It's an organization that was founded in Brussels in 1973 to establish some common processes and standards for financial transactions. SWIFT provides a secure network that allows more than 10,000 financial institutions in 212 different countries to send and receive information about financial transactions to each other. https://transferwise.com/us/blog/everything-you-need-to-know-about-swift-network
2. https://blog.talosintelligence.com/2019/07/sweed-agent-tesla.html?m=1
3. https://www.rarlab.com/rar_file.htm
4. https://fileinfo.com/extension/gz
5. http://www.ntfs.com/bootdisk_quest_isofiles.htm
6. https://whatis.techtarget.com/fileformat/LZH-Compressed-archive-LH-ARC

Infoblox
NEXT LEVEL NETWORKING

Infoblox enables next-level network experiences with its Secure Cloud-Managed Network Services. As the pioneer in providing the world's most reliable, secure and automated networks, we are relentless in our pursuit of network simplicity. A recognized industry leader, Infoblox has 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.

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