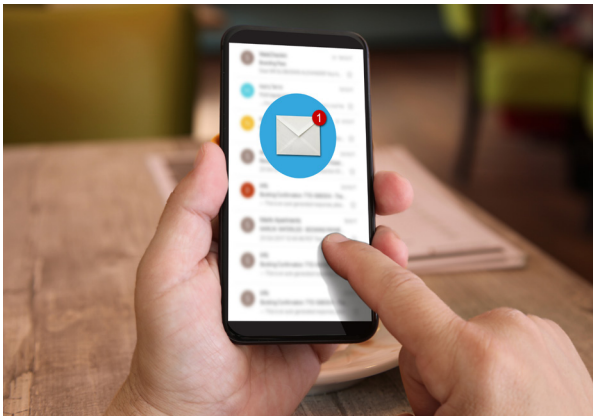
Malspam Sender Spoofing Indian Companies Drops Agent Tesla Keylogger

Author: Victor Sandin



Overview

Between December 13 and 14, Infoblox observed a malicious spam (malspam) email campaign distributing Agent Tesla keylogger[1] via a Microsoft Excel spreadsheet (XLS) with malicious macros. In this campaign, threat actor(s) sent emails spoofing communication from Gopaldas & Sons (also Gopal Das & Sons, both of which represent several large companies in India).

Customer Impact

Agent Tesla is a credential-stealing malware that was first discovered in 2004. It is sold through a subscription-based license on its official website, and according to Threatpost, it has been one of the most popular malware variants in 2020.[2] Agent Tesla's main capabilities include:

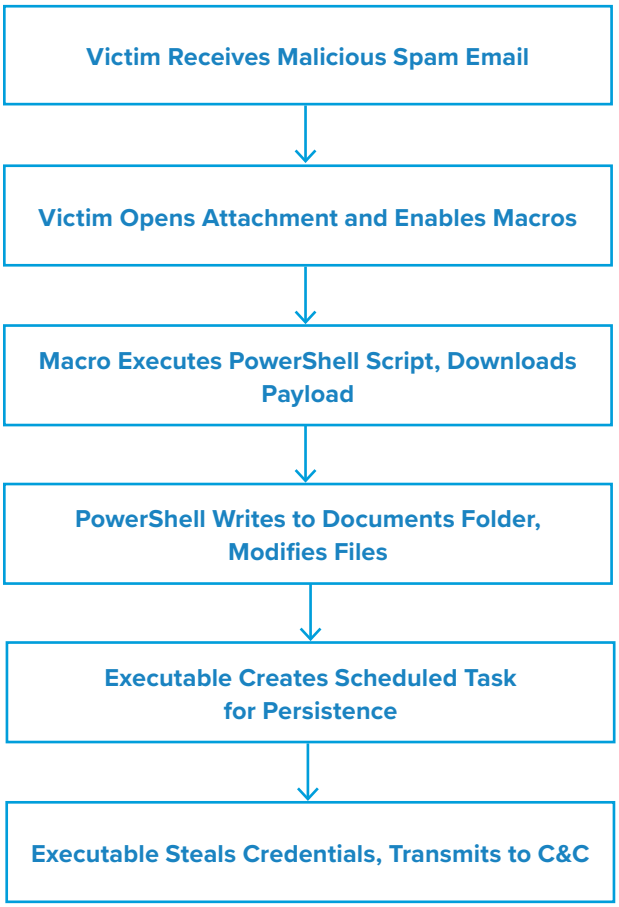
- Keylogging
- Harvesting configuration data and credentials from VPN, FTP and email clients, as well as from web browsers
- Collecting system information
- Transmitting stolen data to its command and control (C&C) via SMTP or FTP
- Evading detection and analysis through strong cryptography protocols

Campaign Analysis

In this campaign, the threat actor(s) distributed emails that impersonated a Gopaldas & Sons purchasing manager with the sender address *lv@gopaldas-sons[.]com* and subject line *Tool kit Lugdivine new order*. The email bodies claimed that the attached file, *RFQ Gopaldas selection.xls*, contained a compiled collection of their products.

Attack Chain

Similar to previous Agent Tesla campaigns,[3] when the user opens the attached XLS file and enables macros, Excel executes a malicious VBA macro. This macro invokes a PowerShell script that downloads the Agent Tesla payload from a controlled C&C server, drops it to the user's Documents folder and executes it.



To maintain persistence, the executable creates a scheduled task that runs every time the system boots up. Finally, it collects credentials from the computer and transmits them to the threat actor's C&C server using SMTP protocol.

Vulnerabilities & Mitigation

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

- Be cautious of emails from unfamiliar senders and inspect unexpected attachments before opening them. Especially if they use commonly-used themes such as shipping or financial documents or advice.
- Configure Microsoft Office to disable macros by default and be cautious if the file's only apparent contents are directions to enable macros.
- Configure firewall rules properly to block unusual traffic.
- Verify important or potentially legitimate attachments with the sender via alternative means (e.g., by phone or in person) before opening them.

Endnotes

1. https://labs.sentinelone.com/agent-tesla-old-rat-uses-new-tricks-to-stay-on-top/
2. https://threatpost.com/agent-tesla-spyware-tricks-arsenal/158284/
3. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--65

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