AZORult Infostealer

Author: Christopher Kim

Overview

From 3 to 4 November, Infoblox observed fashion and beauty-themed malicious spam (malspam) campaigns that delivered AZORult information stealer (infostealer) via Microsoft Excel spreadsheets (XLS) with malicious macros. These spreadsheets used living off the land (LotL) techniques that abused preexisting software on the victim's machine in order to perform malicious tasks.

Customer Impact

The cybersecurity community first discovered AZORult infostealer in 2016.[1] The malware is often bought and sold in Russian dark web forums due to its data-stealing capabilities, which include the following:

- System information (e.g. system language, operating system version, user name and computer name)
- Bitcoin wallets
- Chat software message history
- Email and banking credentials
- Account information from file management software (e.g. FTP clients)
- Browser passwords, cookies and history

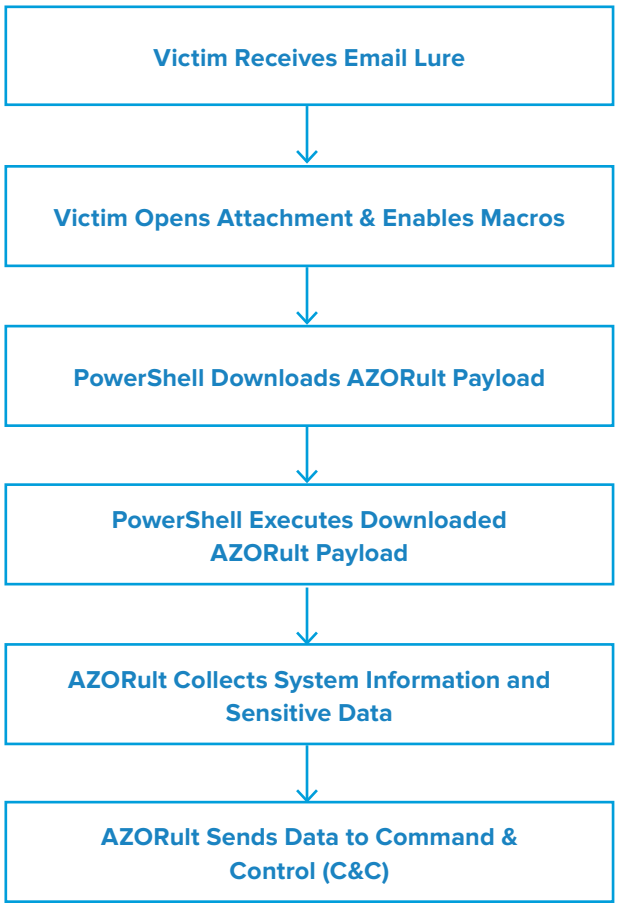
AZORult can also serve as a trojan downloader for other malware payloads.[2] Some versions of AZORult can even establish Remote Desktop Protocol (RDP) connections that allow the attacker to take complete control of the infected system.[3]

Earlier this year, malware campaigns used Coronavirus-themed lures to distribute this infostealer.[4]

Campaign Analysis

The campaigns we observed used fashion and beauty-themed lures with subject lines referencing design patterns. These campaigns also used spoofed email addresses to impersonate legitimate manufacturing businesses based in Portugal and Spain, including health and beauty supplier Mundinter as well as fashion manufacturer Dario Beltran. The email template used for the spoofed Mundinter emails was notably similar to a template used by a recent Agent Tesla campaign.[5] This type of similarity often occurs when different threat actors hire the same botnet to distribute malspam for both of their campaigns.

The emails contained brief and generic messages that encouraged recipients to open the malicious attachment *(FEBEL_List.xls or Patterns.xls)* and reply back for pricing information.



Attack Chain

When the user opened the XLS attachment and enabled macros, the macros in the attachment spawned PowerShell processes to download the AZORult payload from a website. All of the payloads used by the campaigns were hosted on open directories, one of which was publicly available since at least 31 October.

The PowerShell command that downloaded the payload included additional parameters to evade detection and bypass security policies that could block script execution. When the malicious XLS macros ran this PowerShell command, it wrote the AZORult payload to a local file and executed it. AZORult then harvested system information and sensitive credentials. Lastly, AZORult exfiltrated this data by sending HTTP POST requests to its command & control (C&C) server.

Vulnerabilities & Mitigation

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

- Subscribe to Infoblox's Threat Intelligence Feed for DNS Firewall. This feed contains known C&C domains that businesses can add to their Domain Name System (DNS) firewall for protection.
- Enforce strong password policies across all corporate systems and software.
- Apply strong email security solutions that offer spoofing controls such as Sender Policy Framework (SPF), Domain-based Message Authentication Reporting and Conformance (DMARC) and DomainKeys Identified Mail (DKIM).[6]
- Use password manager software to safely store sensitive credentials.
- Update threat signatures for web application firewalls (WAF) to detect malicious HTTP traffic.

Endnotes

1. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--29
2. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--17
3. https://success.trendmicro.com/solution/000146108-azorult-malware-information-kAJ4P000000kEK2WAM
4. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--63
5. https://www.pcrisk.com/removal-guides/18635-mundinter-email-virus
6. https://www.hhs.gov/sites/default/files/maldoc-information-stealer

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