Azorult Malware Analysis

By

Bala Aditya Kota

Background

- A trojan family, first discovered in 2016
- Steals cookies, passwords etc. from the user's browser
- Initially written in Delphi, but later written in C++ and contains AutoIT script (automates windows GUI)
- Also contains SQLite Queries for credit cards, passwords etc.
- Observed to be not persistent – i.e., if no internet connection or unable to resolve command and control domain
- Can be used for impersonation as a service as seen in impaas.ru, which contains nearly 2,60,000 users online
- Primarily targets individual users and gamers, due to the presence of steam gaming distribution, cryptocurrency platforms etc.

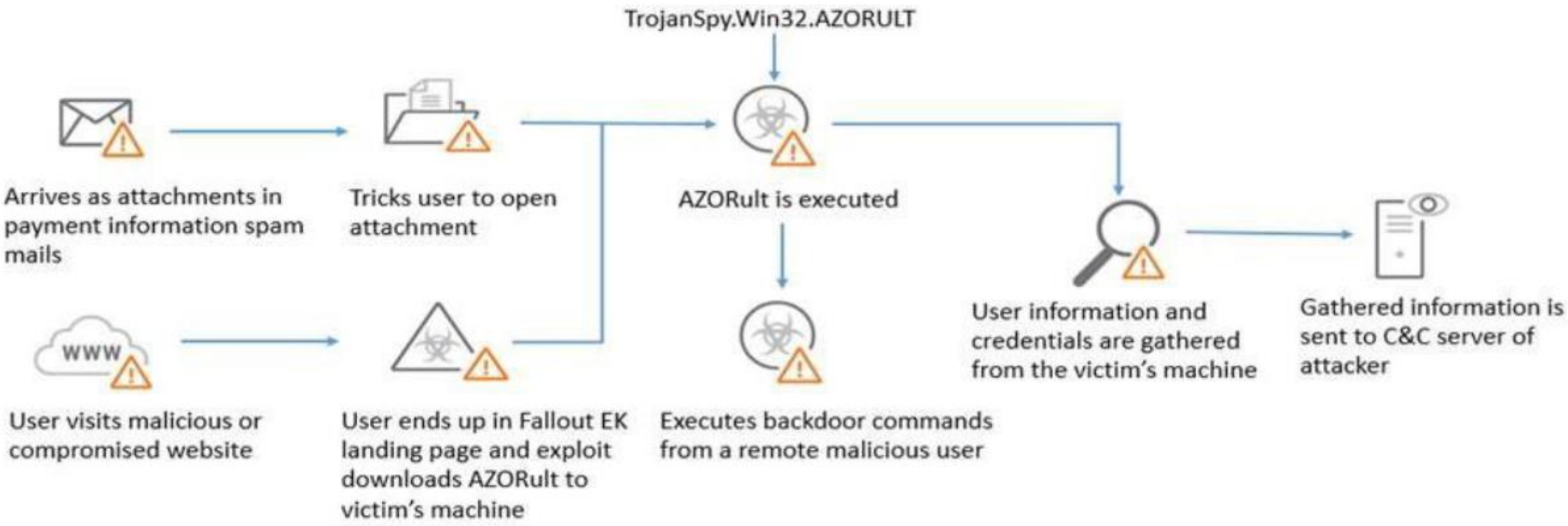
Characteristics

- Propagated usually through phishing
- Needs execution by user
- Event triggered execution to hijack SVCHost process for information stealing
- Gan windows defender permissions, modifies registry for evading detection
- Discovers browser directories for user data and cookies
- Collection of local data and screen capturing – passwords for mails, cryptocurrency wallets, reconnaissance
- Encrypted communication through http, port 80 with command and control
- Observes monitoring tools against hardcoded values

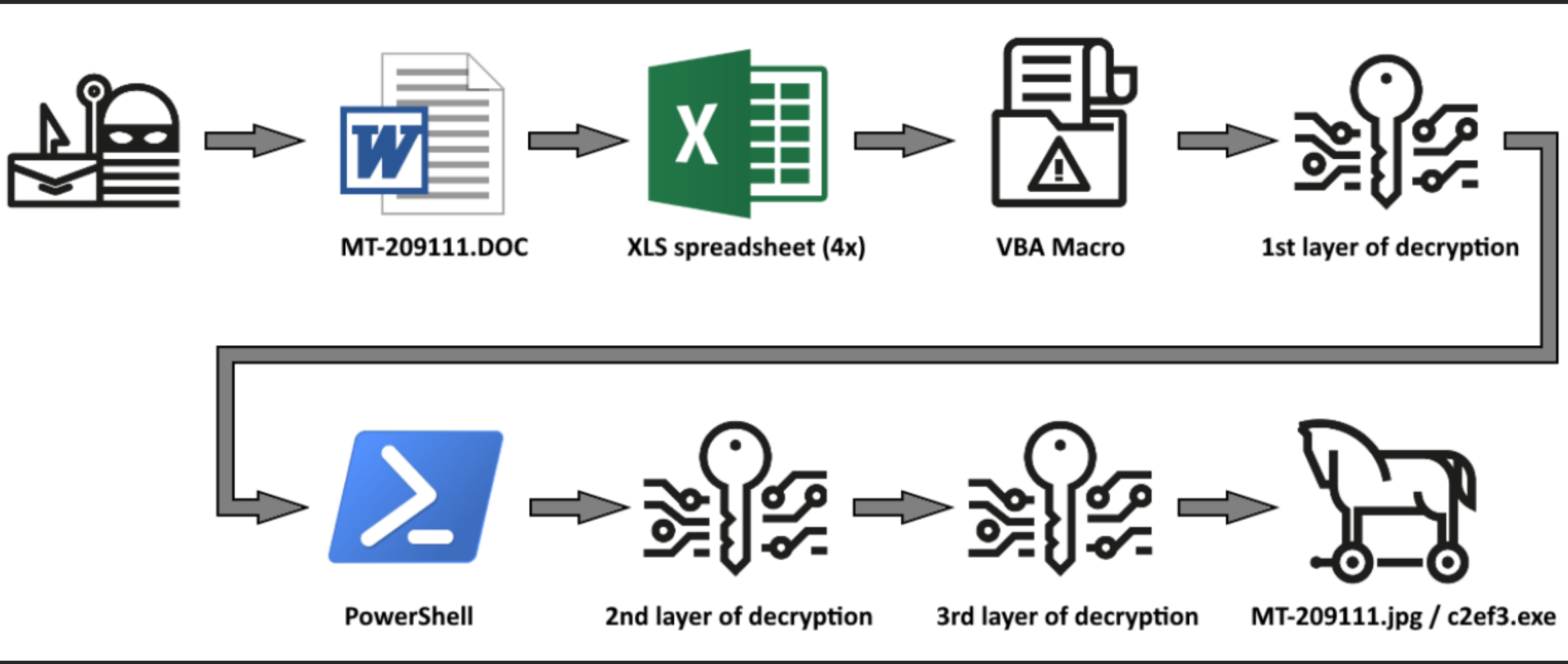
Attack Vectors

- Exploit Kits (especially Fallout Exploit Kit)
- Other malware as droppers - Ramnit, Emotet
- Phishing
- Malspam
- Infected websites
- Malvertisements
- Fake installers
- .iso file, Remote Desktop Protocol (RDP) exploitation

Sample Attack



Recent Variant



Remediation

- Provide social engineering and phishing training to employees.
- Develop and maintain policy on suspicious e-mails for end users; Ensure suspicious e-mails are reported. Ensure emails originating from outside the organization are automatically marked before received.
- Apply patches/updates immediately after release/testing; Develop/maintain patching program if necessary.
- Implement Intrusion Detection System (IDS); Keep signatures and rules updated. Implement spam filters at the email gateways; Keep firewall rules are updated.
- Implement whitelisting technology to ensure that only authorized software is allowed to execute. Implement access control based on the principal of least privilege.
- Conduct system hardening to ensure proper configurations.