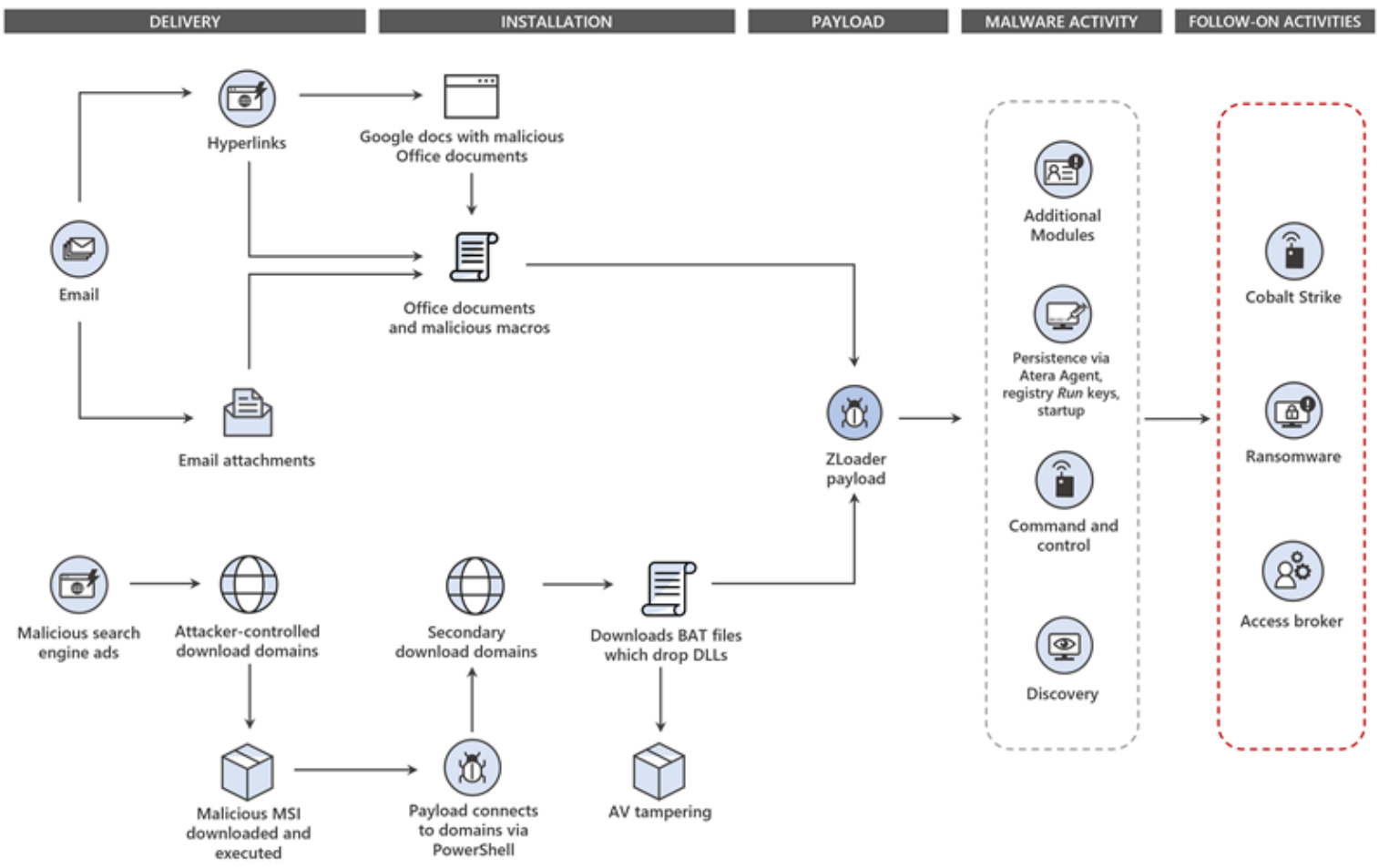
Severity

High

Analysis Summary

The ZLoader, also known as Terdot, is a fork of the iconic Zeus banking trojan, originally found in 2016. The ZLoader has been stealing cookies, passwords, and sensitive information via Microsoft's digital signature verification. It collects login information for online banking sites. When infected users visit a targeted online banking portal, malware dynamically retrieves web injections from its command-and-control (C2) server to alter the page that the user sees so the information entered into the log-in field is transferred to cybercriminals. Their attackers have been observed using invoice-themed spear-phishing infected documents. This wave of ZLoader examples includes files that follow the invoice theme as well. The filenames are commonly "invoice" or "case" followed by four random digits and a peculiar character like ".", "-," or " ." Financial institutions and banks are the most common targets of this trojan.



Microsoft's Digital Crimes Unit (DCU) has now taken legal and technical action against ZLoader. They said, "We obtained a court order from the United States District Court for the Northern District of Georgia allowing us to take control of 65 domains that the ZLoader gang has been using to grow, control and communicate with its botnet. The domains are now directed to a Microsoft sinkhole where they can no longer be used by the botnet's criminal operators. Zloader contains a domain generation algorithm (DGA) embedded within the malware that creates additional domains as a fallback or backup communication channel for the botnet. In addition to the hardcoded domains, the court order allows us to take control of an additional 319 currently registered DGA domains. We are also working to block the future registration of DGA domains."

Impact

- Credential Theft
- Financial Theft
- Data Exfiltration

Indicators of Compromise

Domain Name

- quickbooks[.]pw
- sweepcakesoffers[.]com
- datalystoy[.]com
- teamworks455[.]com

- clouds222[.]com

Remediation

- Search for IOCs in your environment.
- Block all the threat indicators at your respective controls.