BLACKSWAN CYBERSECURITY

THREAT ADVISORY

September 9, 2024

Voldemort Malware Exploiting Google Sheets

SUMMARY

A new malware campaign was recently identified, which leverages Google Sheets as a command-and-control (C2) platform. This campaign impersonates a tax authority from governments agencies across Europe, Asia, and the United States. The threat actors are targeting more than 70 organizations worldwide, utilizing a custom-made tool named Voldemort. This tool is specifically engineered to exfiltrate data and deploy additional malicious payloads. The campaign's scope spans a wide array of sectors, including insurance, aerospace, transportation, academia, finance, technology, industrial manufacturing, healthcare, automotive, hospitality, energy, government, media, telecommunications, and social welfare organizations.

TECHNICAL DETAILS

A recent report by Proofpoint highlights a sophisticated phishing campaign in which attackers craft emails tailored to the geographic location of the targeted organization, utilizing publicly available information. These emails impersonate communications from the organization's national tax authority, purportedly providing updated tax information and including links to relevant documents. When recipients click on the provided link, they are redirected to a landing page hosted on InfinityFree, with the page URL masked by Google AMP Cache. The page features a "Click to view document" button, which, upon interaction, checks the browser's User Agent. If the browser is running on a Windows operating system, the victim is redirected to a search-ms URI (Windows Search Protocol) linked to a URI tunneled through TryCloudflare. Alternatively, users operating on non-Windows platforms are directed to an empty Google Drive URL, which does not deliver any malicious content.

When the victim interacts with the search-ms file, Windows Explorer is activated, presenting a LNK or ZIP file that is deceptively labeled as a PDF document. The use of the search-ms URI in recent phishing campaigns has become increasingly common due to its ability to mislead victims into believing that the file resides locally in their Downloads folder, when in fact it is hosted on an external WebDAV/SMB share. Opening this file initiates the execution of a Python script from another WebDAV share, without actually downloading it to the host machine. This script profiles the victim by collecting system information, all while displaying a decoy PDF to obscure its malicious operations. Concurrently, the script downloads a legitimate Cisco WebEx executable (CiscoCollabHost.exe) alongside a malicious DLL (CiscoSparkLauncher.dll), which subsequently loads the Voldemort malware through DLL side-loading.

Voldemort, a backdoor developed in C, offers a comprehensive array of commands and file management capabilities, including data exfiltration, deployment of additional payloads, and file deletion. A notable aspect of Voldemort is its utilization of Google Sheets as its command and control (C2) server. The malware periodically contacts Google Sheets to receive new commands and uploads exfiltrated data into specific cells within the spreadsheet. These cells are identified using unique identifiers, such as UUIDs, to enable efficient management and isolation of compromised systems. Voldemort communicates with Google Sheets via Google's API, utilizing an embedded client ID, secret, and refresh token stored in its encrypted configuration. This approach provides a highly reliable and resilient C2 channel, minimizing the likelihood of network communication being detected by security systems. Additionally, the pervasive use of Google Sheets in enterprise settings makes it impractical to block the service, thereby enhancing the malware's stealth capabilities.

INDICATORS OF COMPROMISE (IOCs)

- hxxps://pubs[.]infinityfreeapp[.]com/SA150_Notes_2024[.]html
- hxxps://pubs[.]infinityfreeapp[.]com/IRS_P966[.]html
- hxxps://pubs[.]infinityfreeapp[.]com/Notice_pour_remplir_la_N%C2%B0_2044[.]html
- hxxps://pubs[.]infinityfreeapp[.]com/La_dichiarazione_precompilata_2024[.]html

- hxxps://pubs[.]infinityfreeapp[.]com/Steuerratgeber[.]html
- hxxps://od[.]lk/s/OTRfNzQ5NjQwOTJf/test[.]png
- hxxps://od[.]lk/s/OTRfODQ1Njk2ODVf/2044_4765[.]pdf
- hxxps://od[.]lk/s/OTRfODM5Mzc3NjFf/irs-p966[.]pdf
- hxxps://od[.]lk/s/OTRfODM3MjM2NzVf/La_dichiarazione_precompilata_2024[.]pdf
- hxxps://od[.]lk/s/OTRfODQ1NDc2MjZf/SA150_Notes_2024[.]pdf
- hxxps://od[.]lk/s/OTRfODQ1NzA0Mjlf/einzelfragen_steuerbescheinigungen_de[.]pdf
- hxxps://sheets[.]googleapis[.]com:443/v4/spreadsheets/16JvcER[1]0TVQDimWV56syk91IMCYXOvZbW4GTnb947eE/
- hxxps://resource[.]infinityfreeapp[.]com/ABC_of_Tax[.]html
- hxxps://resource[.]infinityfreeapp[.]com/0023012-317[.]html
- hxxps://od[.]lk/s/OTRfODQ4ODE4OThf/logo[.]png
- hxxps://od[.]lk/s/OTRfODQ5MzQ5MzIf/ABC_of_Tax[.]pdf
- hxxp://83[.]147[.]243[.]18/p/
- pants-graphs-optics-worse[.]trycloudflare[.]com
- ways-sms-pmc-shareholders[.]trycloudflare[.]com
- recall-addressed-who-collector[.]trycloudflare[.]com
- invasion-prisoners-inns-aging[.]trycloudflare[.]com
- 0b3235db7e8154dd1b23c3bed96b6126d73d24769af634825d400d3d4fe8ddb9
- 3fce52d29d40daf60e582b8054e5a6227a55370bed83c662a8ff2857b55f4cea
- 561e15a46f474255fda693afd644c8674912df495bada726dbe7565eae2284fb
- 6bdd51dfa47d1a960459019a960950d3415f0f276a740017301735b858019728
- fa383eac2bf9ad3ef889e6118a28aa57a8a8e6b5224ecdf78dcffc5225ee4e1f

RECOMMENDATIONS

- Implement advanced email filtering to detect and block phishing emails, especially those impersonating trusted entities like tax authorities.
- Regularly train employees on how to recognize phishing attempts and suspicious links, particularly those that redirect to unexpected domains.
- Use network monitoring tools to detect unusual traffic patterns, such as unexpected communication with Google Sheets or other cloud-based services.
- Deploy and update endpoint detection and response (EDR) solutions to identify and block malicious scripts, unusual process executions, and unauthorized file activities.
- Limit the execution of macros, scripts, and URI protocols like search-ms, which can be exploited by malware to deliver payloads.
- Ensure that access to cloud services like Google Sheets is monitored and controlled through security policies and access restrictions.
- Keep all software, especially operating systems and productivity tools, updated to protect against known vulnerabilities.

REFERENCES

- https://www.proofpoint.com/us/blog/threat-insight/malware-must-not-be-named-suspected-espionage-campaign-delivers-voldemort
- https://thehackernews.com/2024/08/cyberattackers-exploit-google-sheets.html
- https://www.bleepingcomputer.com/news/security/new-voldemort-malware-abuses-google-sheets-to-store-stolen-data/