Hackers Weaponize Word Files to Deliver DanaBot Malware

Date: 15th May 2024 | Severity: High

Summary

DanaBot is a stealthy and versatile malware that infiltrates computers to steal valuable information for monetization. Unlike ransomware that demands immediate payment, DanaBot operates discreetly, prioritizing long-term persistence and the theft of sensitive data. This well-crafted malware is offered as a malware-as-a-service (MaaS) platform, allowing cybercriminals to customize it for their specific targets.

DanaBot as the latest example of malware focused on persistence and stealing useful information that can later be monetized rather than demanding an immediate ransom from victims. The social engineering in the low-volume DanaBot campaigns we have observed so far has been well-crafted, again pointing to a renewed focus on "quality over quantity" in email-based threats.

Attack Vectors

- DanaBot malware has the capabilities to steal various data from the PC upon infection and can collect information without being connected to the C2 and that the malware takes screenshots and collects PC information and browser account credentials.
- Recent email campaigns distribute DanaBot malware through two document types: those using equation editor exploits and those containing external links, where attackers send emails disguised as job applications with a malicious Word document attached. The document itself doesn't contain malware but instead tricks the user into clicking an external link that initiates the DanaBot infection process.
- The deployment of DanaBot stealer involves multiple stages from downloading to execution and involves different sources for each stage payload. The first stage payload is in the malicious attachment which includes documents and script files with obfuscated content, leading to the source of second stage payload.
- DanaBot includes banking site web injections and stealer functions. It consists of a downloader component that downloads an encrypted file containing the main DLL. The DLL, in turn, connects using raw TCP connections to port 443 and downloads additional modules including:
  VNCDLL.dll - "VNC"
  StealerDLL.dll - "Stealer"
  ProxyDLL.dll - "Sniffer".

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• ee1e5b80a1d3d47c7703ea2b6b64ee96283ab3628ee4fa1fef6d35d1d9051e9f • 28fd189dc70f5bab649e8a267407ae85 • e29e4a6c31bd79d90ab2b89f57075312 • 0bb0ae135c2f4ec39e93dcf66027604d • 5c67e2d3e488622d200fbb8bf3418206dfe05a5b • e4bba16c2aa6563e30a7eafccbcb5f43e4b72f68 • 6bdb302e1dd3a6af6e22f319da1898b46eeb9c55 • 1f406eed3f646a1a30cfe95667e1dfa3884763e9 • 52c99b8b5c5d6934ee8cf8d15c84a8f7a12a57ed • f5999bffa70a09d8456c49e3f6fc6bfd6866d71b • 3b93128329c38c48f427d31f51401deda79dbce6 • 929b101cd60f9b02b9e8b11b891c34918accfb7a • c6724845350b1745f02d1430a5d27578a44a9e19 • ef054f54df0fa67fc454bf8894c643e44c28ec3a • 6d54a64b57b9fdcffdab43323b1755356a136d42 • 608399379d28895ba7a35f983440f199fb66f9d7 • 29c8478a7c47926146955982de6bb2f64361b82d • 5742d4a59148a395c5eddae41c469f0894a7f277 • 7df458e26a20581d2d9fd78fdbf2b450bdbb643d • 781c63cf4981fa6aff002188307b278fac9785ca66f0b6dfcf68adbe7512e491 • bb525dc6b7a7ebefd040e01fd48d7d4e178f8d9e5dec9033078ced4e9aa4e21 • 9c27405cf926d36ed8e247c17e6743ac00912789efe0c530914d7495de1e21c • 97e093f2e0bf6dec8392618722dd6b4411088fe752bedece910d11fffe0288a2 • aee22a35cbdac3f16c3ed742c0b1bfe9739a13469cf43b36fb2c63565111028c • d9471b038c44619739176381815bfa9a13b5ff77021007a4ede9b146ed2e04c • eb51f3b6b62c69672dbeced9ce2252675db44222 • 090f2c5abb85a7b115dc25ae070153e4e958ae4e1bc2310226c05cd3e9429446 • 0ac5030e2171914f43e0769cb10b602683ccc9da09369bcd4b80da6edb8be80e • 378d220bc863a527c2bca204daba36f10358e058df49ef088f8b1045604d9d05 • db03a34684feab7475862080f59d4d99b32c74d3a152a53b257fd1a443e8ee77 • dedbc21afc768d749405de535f9b415baaf96f7664ded55d54829a425fc61d7e • e99f3517a36a9f7a55335699cfb4d84d08b042d47146119156f7f3bab580b4d7 • edeacd49aff3cfea35d593e455f7caca35ac877ad6dc19054458d41021e0e13a • f9c69e79e7799df31d6516df70148d7832b121d330beebe52cff6606f0724c62 • e7ff6a7ac5bfb0bb29547d413591abc7628c7d5576a3b43f6d8e5d95769e553a • 3b63ea8b6f9b2aa847faa11f6cd3eb281abd9b9cceedb570713c4d78a47de567 • 60c4b6c230a40c80381ce283f64603cac08d3a69ceea91e257c17282f66ceddc • 88573297f17589963706d9da6ced7893eacbdc7d6bc43780e4c509b88ccd2aef • 47168fa869331faf08db71690f24e567c5cdf1f01cc5e2a8d08c93d282c9 • a189963ff252f547fddfc394c81f6e9d49eac403c32154eebe06f4cddb5a2a22 • aa29a8af8d615b1dd9f52fd49d42563fbeafa35ff0ab1b4afc4cb2b2fa54a119 • d98cd810d568f338f16c4637e8a9cb01ff69ee1967f4cfc004de3f283d61ba81
URLs	• http[:]//5.252.21.207/share/escape.msi • https[:]//popfealt.one/live/ • https[:]//aytobusesre.com/live/ • https[:]//zumkoshapsret.com/live/ • https[:]//scifimond.com/live/ • https[:]//aprettopizza.world/live/ • https[:]//sluitionsbad.tech/live/ • https[:]//grebiunti.top/live/

Domain	• titnovacrion[.]top • sokingscrosshotel[.]com • nimeklroboti[.]info • frotneels[.]shop
IP Address	• 80.66.75[.]44 • 141.8.192[.]151 • 199.36.158[.]100 • 192.210.198[.]12 • 5.42.65[.]101 • 107.175.229[.]139 • 104.250.180[.]178

Recommendation

- Secure remote access functionalities such as remote desktop protocol.
- Enable multi-factor authentication when accessing banking applications.
- Be highly caution while downloading Word documents from emails sent by unknown sources.
- Implement an additional layer of security for blocking installations of unknown executables or applications.
- Monitor network traffic for suspicious activities, such as C&C communications and irregular network data spikes.
- Implement behavior-based monitoring to detect unusual activity patterns, such as suspicious processes attempting to make unauthorized network connections.

NOTE: The recommended settings/controls should be implemented after due shall betested on Pre-Prod or test environment before implementing. diligence and impactanalysis.

Reference Links

- https://cybersecuritynews.com/danabot-malware-via-weaponized-word-files/
- https://malware.news/t/distribution-of-danabot-malware-via-word-files-detected-by-ahnlab-edr/81872
- https://www.cyfirma.com/research/danabot-stealer-a-multistage-maas-malware-re-emerges-with-reduced-detectability/