CarnavalHeist Banking Trojan Targeting Brazilian Users

Date: 04th June 2024 | Severity: High

Summary

CarnavalHeist malware is of Brazilian origin and primarily targets Brazilian users based on our observations of the Portuguese language being used throughout all aspects of the infection chain and the malware itself, including the use of Brazilian slang to describe some bank names, and a notable lack of other language variants thus far. The command and control (C2) infrastructure exclusively uses the BrazilSouth availability zone on Microsoft Azure to control infected machines, and they specifically target prominent Brazilian financial institutions.

Attack Vectors

- The infection chain begins with a financial themed mail through which the recipient is lured into downloading an invoice (named as “Nota Fiscal” which is Portuguese for invoice).
- The malicious link uses the IS.GD URL shortener service to redirect users to the first-stage payload.
- This URL redirects the user to the server hosting the fake web page where the users are supposed to download their invoice. We have observed different domains being used in this step, but all contain references to “Nota Fiscal Eletrônica,” the Portuguese term for invoice.
- The actual download is a malicious LNK file which leads to further downloads and executions of script components which are responsible for delivering the final malicious payload.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• c300749ea44f886be1887b3e19b946efbdbbc3e1bf3e416c78cfbff8d23bf70a • 1b4f44a00f61b3e0c8cd6c3125f03b6d4897d6ab90c8a6dc899ed96acee80dd6 • 8424e76c9a4ee7a6d7498c2f6826fcde390616dc65032bebf6b2a6f8fbf4a535 • d9877dc1ba0f977d100e687da59c216454d27e3988532652ac8f6331debbd071 • 0d94547a0b8f9795e97e2a4a58b0ece65b4ea4b6e6019cbc96e1c79f373b4587 • f848c0f66afc7b5a10f060c1db129529a974ae0ad71a767f7c7793351bb7ca04

	• f2db799d892f2a7ac82bfa15826e74d778abdfa153ccafb9db1fdf56a0248a40 • 5782b9bc96ce5ad011c122496ff0ff0dc08d6444c6d2e98606ada82130d5f21a • 19c02c5724622be4eedff95633f3fbaa604449aa50cc0761693bb8adb1e8cf97 • b8b3963967232916cd721a22c80c11cd33057bd5629dcfa3f4b03d8a6dbf1403 • 883c49b7c869019951eff94699480a7ecc97c9c45060a15797ecbd5fce060d26 • e7aa64726783ec6f7249483e984ae20b31a091a488a3ed0f83c210702c506d20
URLs	• hxxps[://]is[.]gd/38qeon?0177551.5510 • hxxps[://]is[.]gd/ROnj3W?0808482.5176 • hxxps[://]notafiscaleletronica[.]nf-e[.]pro/danfe/?notafiscal=00510242.500611 • hxxps[://]nota-fiscal[.]nfe-digital[.]top/nota-estadual/?notafiscal=00792011.977347 • hxxps[://]nfe-visualizer[.]app[.]br/notas/?notafiscal=000851113082.35493424000 • hxxp[://]adobe-acrobat-visualizer[.]brazilsouth[.]cloudapp[.]azure[.]com/Documentos
IP	• 104[.]41[.]51[.]80 • 191[.]239[.]116[.]217 • 191[.]239[.]123[.]241 • 191[.]233[.]241[.]96 • 191[.]234[.]212[.]140 • 191[.]235[.]233[.]246 • 4[.]203[.]105[.]118 • 191[.]233[.]248[.]170

Recommendation

- Submit the File Hash to the Antivirus team to update their database with the file hashes.
- Submit the Domains to the Network team to update their database with the Domains.
- Secure RDP ports to prevent threat actors from abusing and leveraging RDP tools.
- Prioritize remediating known exploited vulnerabilities.
- Implement EDR solutions to disrupt threat actor memory allocation techniques.
- Make regular backups of important and critical files.
- Avoid browsing the unsafe websites, clicking on suspicious links, or opening unknown email attachments.
- Update and Patch operating system, applications, and security software's up to date with latest patches.

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

Reference Link

- https://blog.talosintelligence.com/new-banking-trojan-carnavalheist-targets-brazil/