Beat: Technology

Stolen Images Campaign Ends in Conti Ran

Cybersecurity Alert: From Alientvault

New York City, 04.04.2022, 16:07 Time

Alienvault.com - Alert by Alienvault.com: Currently active cyber threat. The pulse report from Alienvault indicates the current cyber threat has been active within the past 9 hours as of the publishing time of this report 12:40 pm EST.

In this intrusion from December 2021, the threat actors utilized IcedID as the initial access vector. IcedID is a banking trojan that first appeared in 2017, usually, it is delivered via malspam campaigns and has been widely used as an initial access vector in multiple ransomware intrusions. Upon execution of the IcedID DLL, discovery activity was performed which was followed by the dropping of a Cobalt Strike beacon on the infected host. Along the way, the threat actors installed remote management tools such as Atera and Splashtop for persisting in the environment. While remaining dormant most of the time, the adversary deployed Conti ransomware on the 19th day (shortly after Christmas), resulting in domain wide encryption.

REFERENCE:
https://thedfirreport.com/2022/04/04/stolen-images-campaign-ends-in-conti-ransomware/
TAGS:
Conti, Ransomware, IcedID, malspam
ADVERSARY:
Conti
MALWARE FAMILY:
Conti

ATT&CK IDS:
T1187 - Forced Authentication, T1566 - Phishing, T1547 - Boot or Logon Autostart Execution, T1114 - Email Collection, T1003 - OS Credential Dumping, T1018 - Remote System Discovery, T1021 - Remote Services, T1047 - Windows Management Instrumentation, T1049 - System Network Connections Discovery, T1053 - Scheduled Task/Job, T1055 - Process Injection, T1059 - Command and Scripting Interpreter, T1068 - Exploitation for Privilege Escalation, T1071 - Application Layer Protocol, T1082 - System Information Discovery, T1083 - File and Directory Discovery, T1087 - Account Discovery, T1218 - Signed Binary Proxy Execution, T1219 - Remote Access Software, T1482 - Domain Trust Discovery, T1486 - Data Encrypted for Impact, T1518 - Software Discovery, T1562 - Impair Defenses, T1569 - System Services, T1614 - System Location Discovery

All data provided by OTX.ALIENVAULT.COM

Article online:
https://www.uspa24.com/bericht-20365/stolen-images-campaign-ends-in-conti-ran.html

Editorial office and responsibility:
V.i.S.d.P. & Sect. 6 MDStV (German Interstate Media Services Agreement):

Exemption from liability:
The publisher shall assume no liability for the accuracy or completeness of the published report and is merely providing space for the submission of and access to third-party content. Liability for the content of a report lies solely with the author of such report.

Editorial program service of General News Agency:
UPA United Press Agency LTD
483 Green Lanes
UK, London N13NV 4BS
contact (at) unitedpressagency.com
Official Federal Reg. No. 7442619