Code insights

The PowerShell script `pwncrypt.ps1` simulates a ransomware attack. It begins by defining a log file path and a function to write log messages. It then attempts to encrypt files within a randomly selected user's Desktop directory.

The script uses a hardcoded AES key and initialization vector (IV) to encrypt text content. It identifies user directories under `C:\Users`, excluding standard system accounts. A random user is selected, and the script targets the user's Desktop folder.

The script defines a set of fake company data stored as strings. It cleans up pre-existing files matching a specific pattern in the destination folder. It then creates new files with the fake content. The content is encrypted, and the script proceeds to replace the original with the encrypted version. Note that the script first creates the real file, then the temporary file, and proceeds to convert the temporary file back into the original file.

Finally, it drops a ransom note named `____________decryption-instructions.txt` on the user's Desktop with a Bitcoin address. All activities, along with error messages, are logged to a file specified by `$logFilePath`.

Show less

Crowdsourced AI

⚠ NICS Lab flags this file as malicious

The provided PowerShell script is designed to perform malicious activities consistent with ransomware behavior. It begins by defining a log file path and includes a function for logging messages, which indicates an intention to track its operations. The script then generates an encryption key and an initialization vector (IV) for AES encryption.

The core functionality of the script involves the following steps:

1. User Directory Enumeration: It retrieves user directories from `C:\Users`, *excluding system and default accounts. This suggests that it targets specific user profiles on the machine.*

2. File Creation and Encryption: The script creates fake files containing sensitive-looking information (e.g., employee records, project lists, financial data) in the selected user's Desktop folder. These files are named with a random prefix followed by `_pwncrypt.csv`.

3. Encryption Process: Each fake file's content is encrypted using the AES algorithm, and the original plaintext files are deleted after encryption. The encrypted files are then moved to a temporary directory before being renamed back to their original location.

4. Decryption Instructions: Finally, the script writes decryption instructions to a text file on the Desktop, demanding a ransom payment in Bitcoin for the decryption key. This is a clear indication of ransomware activity, as it aims to extort money from the victim.

Overall, the script exhibits all characteristics of ransomware, including file encryption, creation of misleading documents, and demands for payment, thus classifying it as malicious.
Show less

Security vendors' analysis Do you want to automate checks?

Acronis (Static ML)	✓ Undetected
AhnLab-V3	✓ Undetected
AliCloud	✓ Undetected
ALYac	✓ Undetected
Antiy-AVL	✓ Undetected
Arcabit	✓ Undetected
Avast	✓ Undetected
AVG	✓ Undetected
Avira (no cloud)	✓ Undetected
Baidu	✓ Undetected
BitDefender	✓ Undetected
Bkav Pro	✓ Undetected
ClamAV	✓ Undetected
CMC	✓ Undetected
CrowdStrike Falcon	✓ Undetected
CTX	✓ Undetected
Cynet	✓ Undetected
DrWeb	✓ Undetected
Emsisoft	✓ Undetected

eScan	✓	Undetected
ESET-NOD32	✓	Undetected
Fortinet	✓	Undetected
GData	✓	Undetected
Google	✓	Undetected
Gridinsoft (no cloud)	✓	Undetected
Huorong	✓	Undetected
Ikarus	✓	Undetected
Jiangmin	✓	Undetected
K7AntiVirus	✓	Undetected
K7GW	✓	Undetected
Kaspersky	✓	Undetected
Kingsoft	✓	Undetected
Lionic	✓	Undetected
Malwarebytes	✓	Undetected
MaxSecure	✓	Undetected
Microsoft	✓	Undetected
NANO-Antivirus	✓	Undetected
Panda	✓	Undetected
QuickHeal	✓	Undetected
Rising	✓	Undetected
Sangfor Engine Zero	✓	Undetected
Skyhigh (SWG)	✓	Undetected
Sophos	✓	Undetected
SUPERAntiSpyware	✓	Undetected
Symantec	✓	Undetected
TACHYON	✓	Undetected
Tencent	✓	Undetected
Trellix (ENS)	✓	Undetected
TrendMicro	✓	Undetected
TrendMicro-HouseCall	✓	Undetected
Varist	✓	Undetected
VBA32	✓	Undetected
VIPRE	✓	Undetected
VirIT	✓	Undetected
ViRobot	✓	Undetected
WithSecure	✓	Undetected
Xcitium	✓	Undetected
Yandex	✓	Undetected

Zillya	✓	Undetected
ZoneAlarm by Check Point	✓	Undetected
Zoner	✓	Undetected
Alibaba	⊘	Unable to process file type
Arctic Wolf	⊘	Unable to process file type
Avast-Mobile	⊘	Unable to process file type
BitDefenderFalx	⊘	Unable to process file type
DeepInstinct	⊘	Unable to process file type
Elastic	⊘	Unable to process file type
McAfee Scanner	⊘	Unable to process file type
Palo Alto Networks	⊘	Unable to process file type
SecureAge	⊘	Unable to process file type
SentinelOne (Static ML)	⊘	Unable to process file type
Symantec Mobile Insight	⊘	Unable to process file type
TEHTRIS	⊘	Unable to process file type
Trapmine	⊘	Unable to process file type
Trustlook	⊘	Unable to process file type
Webroot	⊘	Unable to process file type