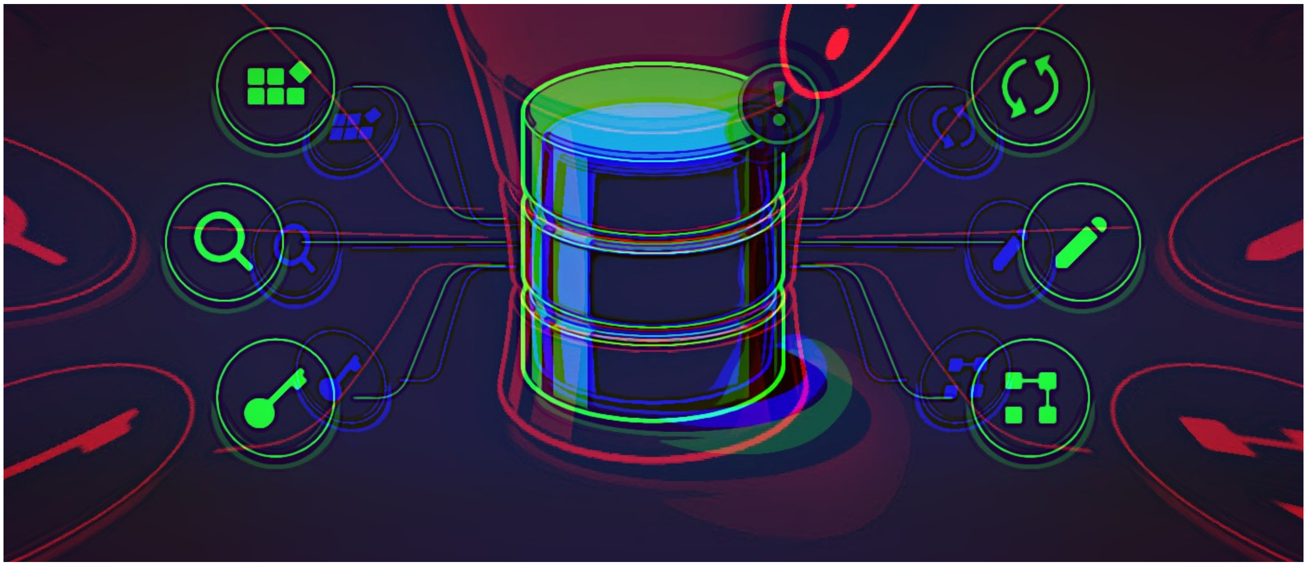
# Ransomware gang's script shows exactly the files they're after

bleepingcomputer.com/news/security/ransomware-gangs-script-shows-exactly-the-files-theyre-after/

Lawrence Abrams

By
Lawrence Abrams

- August 24, 2021
- 02:16 PM
- 0



A PowerShell script used by the Pysa ransomware operation gives us a sneak peek at the types of data they attempt to steal during a cyberattack.

When ransomware gangs compromise a network, they usually start with limited access to a single device.

They then use various tools and exploits to steal other credentials used on the Windows domain or gain elevated privileges on different devices.

Once they gain access to a Windows domain controller, they search for and steal data on the network before encrypting devices.

The threat actors use this stolen data in two ways.

The first is to generate a ransom demand based on company revenue and whether they have insurance policies. The second is to scare the victims into paying a ransom because the gang will leak the data.

## Searching for valuable data

Yesterday, MalwareHunterTeam shared a PowerShell script with BleepingComputer used by the Pysa ransomware operation to search for and exfiltrate data from a server.

This script is designed to scan each drive for data folders whose names match certain strings on a device. If a folder matches the search criteria, the script will upload the folder's files to a remote drop server under the threat actor's control.

Of particular interest are the 123 keywords that the script searches for, which give us a glimpse into what the ransomware gang considers valuable.

As we would expect, the script seeks out files related to the companies financials or personal information, such as audit, banking information, login credentials, tax forms, student information, social security numbers, and SEC filings.

However, it also looks for more intriguing keywords that could be particularly harmful to a company if leaked, such as folders containing the words 'crime', 'investigation', 'fraud', 'bureau', 'federal', 'hidden', 'secret', 'illegal', and 'terror.'

The full list of 123 keywords targeted by the threat actors' script is listed in the table below.

| | | | |
|---|---|---|---|
| 941 | confident | Info | RRHH |
| 1040 | Crime | insider | saving |
| 1099 | claim | Insurance | scans |
| 8822 | Terror | investigation | sec |
| 9465 | Confidential*Disclosure | IRS | secret |
| 401K | contact | ITIN | security |
| 4506-T | contr | K-1 | studen |
| ABRH | CPF | letter | seed |
| Audit | CRH | List | Signed |
| Addres | Transact | Login | sin |
| agreem | DDRH | mail | soc |
| Agreement*Disclosure | Demog | NDA | SS# |
| ARH | Detail | Numb | SS-4 |
| Assignment | Disclosure*Agreement | Partn | SSA |

| | | | |
|---|---|---|---|
| balanc | Disclosure*Confidential | passport | SSN |
| bank | DRH | passwd | Staf |
| Bank*Statement | emplo | password | statement |
| Benef | Enrol | pay | Statement*Bank |
| billing | federal | payment | SWIFT |
| budget | Finan | payroll | tax |
| bureau | finance | person | Taxpayer |
| Brok | Form | Phone | unclassified |
| card | fraud | privacy | Vend |
| cash | government | privat | W-2 |
| CDA | hidden | pwd | w-4 |
| checking | hir | Recursos*Humanos | W-7 |
| clandestine | HR | report | W-8BEN |
| compilation | Human | Resour | w-9 |
| compromate | i-9 | resurses*human | W-9S |
| concealed | illegal | RHO | |
| confid | important | routing | |

It does not make sense to change your folder names, so they do not include these strings, as the threat actors will likely perform manual sweeps of data.

However, knowing what types of data a ransom gang is searching for gives you a better indication of how ransomware gangs will attempt to extort their victims.

Pysa is not the only one searching for particular files after breaching a network.

Earlier this month, an angry Conti affiliate leaked the training material for the ransomware operation.

This training material told affiliates to immediately search for data containing the following keywords after they gained control of a Windows domain controller.

```
cyber
policy
insurance
endorsement
supplementary
underwriting
terms
bank
2020
2021
Statement
```

Once again, this illustrates how vital data theft is to a ransomware attack and how important it is to safeguard it adequately.

## Related Articles:

Industrial Spy data extortion market gets into the ransomware game

Quantum ransomware seen deployed in rapid network attacks

Snap-on discloses data breach claimed by Conti ransomware gang

Shutterfly discloses data breach after Conti ransomware attack

Windows 11 KB5014019 breaks Trend Micro ransomware protection

- Data Exfiltration
- PYSA
- Ransomware
- Theft

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

## You may also like: