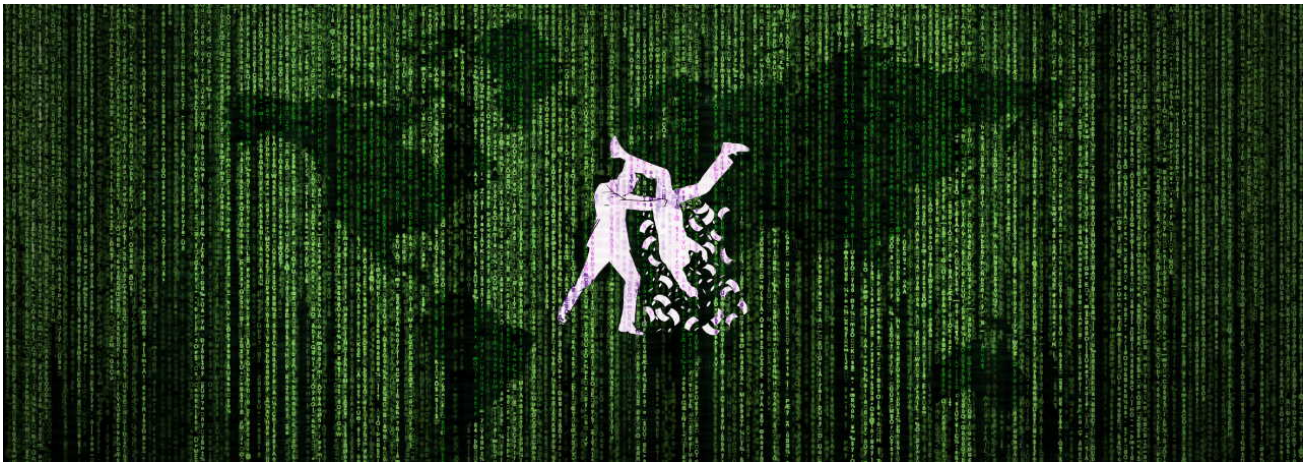
New Ryuk Info Stealer Targets Government and Military Secrets

bleepingcomputer.com/news/security/new-ryuk-info-stealer-targets-government-and-military-secrets/

Lawrence Abrams

By
Lawrence Abrams

- January 24, 2020
- 02:12 PM
- 0



A new version of the Ryuk Stealer malware has been enhanced to allow it to steal a greater amount of confidential files related to the military, government, financial statements, banking, and other sensitive data.

In September 2019, we reported on a new malware that included references to the Ryuk Ransomware and was used to steal files if the file's name matched certain keywords.

It is not known if this tool is created by the Ryuk Ransomware actors to be used for data exfiltration before encrypting a victim's computer or if another actor simply borrowed from the ransomware's code.

"It is likely the same actor with the access to the earlier Ryuk version who repurposed the code portion for this stealer," Head of SentinelLabs Vitali Kremez told BleepingComputer.

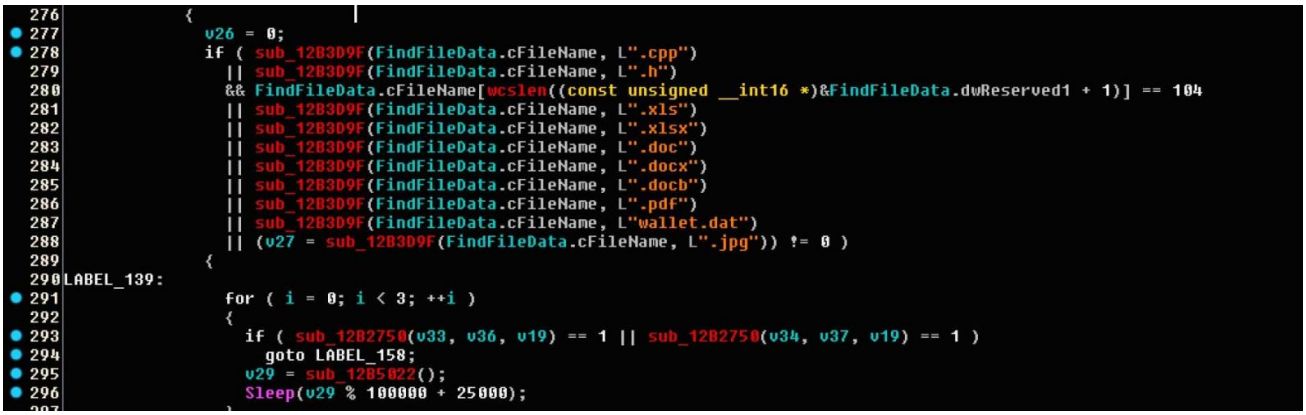
What we do know is that the malware is targeting very specific keywords that could be disastrous for governments, military operations, and law enforcement cases if the stolen files are exposed.

New features added to the Ryuk Stealer

A new variant of the Ryuk Stealer malware was discovered today by MalwareHunterTeam that adds a new file content scanning feature and additional keywords that it targets for theft.

In the previous version, the Ryuk Stealer would scan a computer's files for Word (docx) and Excel (xlsx) documents.

According to Kremez, this new version of the stealer will look for an additional seven file types related to C++ source code, further Word and Excel document types, PDFs, JPG image files, and cryptocurrency wallets.



```
276           {
277             v26 = 0;
278             if ( sub_12B3D9F(FindFileData.cFileName, L".cpp")
279               || sub_12B3D9F(FindFileData.cFileName, L".h")
280               && FindFileData.cFileName[wcslen((const unsigned __int16 *)&FindFileData.dwReserved1 + 1)] == 104
281               || sub_12B3D9F(FindFileData.cFileName, L".xls")
282               || sub_12B3D9F(FindFileData.cFileName, L".xlsx")
283               || sub_12B3D9F(FindFileData.cFileName, L".doc")
284               || sub_12B3D9F(FindFileData.cFileName, L".docx")
285               || sub_12B3D9F(FindFileData.cFileName, L".docb")
286               || sub_12B3D9F(FindFileData.cFileName, L".pdf")
287               || sub_12B3D9F(FindFileData.cFileName, L"wallet.dat")
288               || (v27 = sub_12B3D9F(FindFileData.cFileName, L".jpg")) != 0 )
289             {
290 LABEL_139:
291               for ( i = 0; i < 3; ++i )
292               {
293                 if ( sub_12B2750(v33, v36, v19) == 1 || sub_12B2750(v34, v37, v19) == 1 )
294                   goto LABEL_158;
295                 v29 = sub_12B5022();
296                 Sleep(v29 % 100000 + 25000);
```

Targeted Extension

The full list of targeted extensions are:

```
.cpp
.h
.xls
.xlsx
.doc
.docx
.pdf
wallet.dat
.jpg
```

If a file matches one of the above extensions, the stealer will check the contents of the file and see if they contain one of the 85 keywords listed below.

```
'personal', 'securityN-CSR10-SBEDGAR', 'spy', 'radar', 'agent', 'newswire',
'marketwired', '10-Q', 'fraud', 'hack', 'defence', 'treason', 'censored', 'bribery',
'contraband', 'operation', 'attack', 'military', 'tank', 'convict', 'scheme',
'tactical', 'Engeneering', 'explosive', 'drug', 'traitor', 'suspect', 'cyber',
'document', 'embeddedspy', 'radio', 'submarine', 'restricted', 'secret', 'balance',
'statement', 'checking', 'saving', 'routing', 'finance', 'agreement', 'SWIFT',
'IBAN', 'license', 'Compilation', 'report', 'secret', 'confident', 'hidden',
'clandestine', 'illegal', 'compromate', 'privacy', 'private', 'contract',
'concealed', 'backdoorundercover', 'clandestine', 'investigation', 'federal',
'bureau', 'government', 'security', 'unclassified', seed', 'personal', 'confident',
'mail', 'letter', 'passport', 'victim', 'court', 'NATO', 'Nato', 'scans', 'Emma',
'Liam', 'Olivia', 'Noah', 'William', 'Isabella', 'James', 'Sophia', 'Logan',
'Clearance'
```

In addition, the stealer will check if the filename contains any of the following 55 keywords:

```
'SECURITY', 'N-CSR', '10-SB', 'EDGAR', ' spy ', 'radar', 'censored', 'agent',
'newswire', 'marketwired', '10-Q', 'fraud', 'hack', 'NATO', 'Nato',
'convictMilitary', 'military', 'submarine', 'Submarinesecret', 'Secret', 'scheme',
'tactical', 'Engeneering', 'explosive', 'drug', 'traitor', 'embeddedspy', 'radio',
'suspect', 'cyber', 'document', 'treasonrestricted', 'private', 'confident',
'important', 'pass', 'victim', 'court', 'hidden', 'bribery', 'contraband',
'operation', 'undercover', 'clandestine', 'investigation', 'federal', 'bureau',
'government', 'security', 'unclassified', 'concealed', 'newswire', 'marketwired',
'Clearance'
```

When a matching document is found, the malware will upload it to an FTP site that is under the attacker's control. The two embedded FTP sites currently being used by the malware are down.

Targeting highly sensitive documents

As you can see, the targeted keywords are related to sensitive subjects for a variety of data categories such as:

- **Banking**: 'SWIFT', 'IBAN', 'balance', 'statement', 'checking', 'saving', 'routing'
- **Finance**: 'N-CSR', '10-SB', 'EDGAR', 'newswire', 'marketwired', '10-Q'
- **Law Enforcement**: 'clandestine', 'investigation', 'federal', 'bureau', 'government', 'security', 'victim', 'court'
- **Military**: 'NATO', 'operation', 'attack', 'spy', 'radar', 'tactical', 'tank', 'submarine'
- **Personal**: 'personal', 'passport', 'Emma', 'Liam, 'Olivia, 'Noah', 'William', 'Isabella', 'James', 'Sophia', 'Logan'

The names in the Personal category are taken from the United States Social Security Department's list of top baby names.

Some of the new search words that were added since the latest version include 'treason', 'NATO', 'convict', 'traitor', 'embeddedspy', 'cyber', 'submarine', 'Submarinesecret', 'contraband', 'radio', 'suspect', 'operation', and 'bribery.'

Based on the targeted keywords in this malware, it looks like the attackers are looking for confidential information to sell to foreign adversaries, corporations, or to be used as blackmail.

At this time, we do not know how this malware is being distributed and if its bundled with ransomware attacks or used independently.

With data exfiltration becoming more common and increasingly being used by ransomware, it is important to make sure you have good security measures in place to protect your network from compromise.

This includes being careful of phishing emails with malicious attachments, do not make Remote Desktop Services publicly accessible, make sure all software and operating systems are updated, and make sure to use security software and good password policies.

Related Articles:

New Industrial Spy stolen data market promoted through cracks, adware

New ChromeLoader malware surge threatens browsers worldwide

Industrial Spy data extortion market gets into the ransomware game

New ERMAC 2.0 Android malware steals accounts, wallets from 467 apps

Popular Python and PHP libraries hijacked to steal AWS keys

- Data Exfiltration
- Malware
- Ryuk
- Ryuk Stealer
- Steal

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

You may also like: