Cynet Detection Report: Ragnar Locker Ransomware

Archived: 2026-04-06 03:21:29 UTC

Written by: Ben Gold

EXECUTIVE SUMMARY

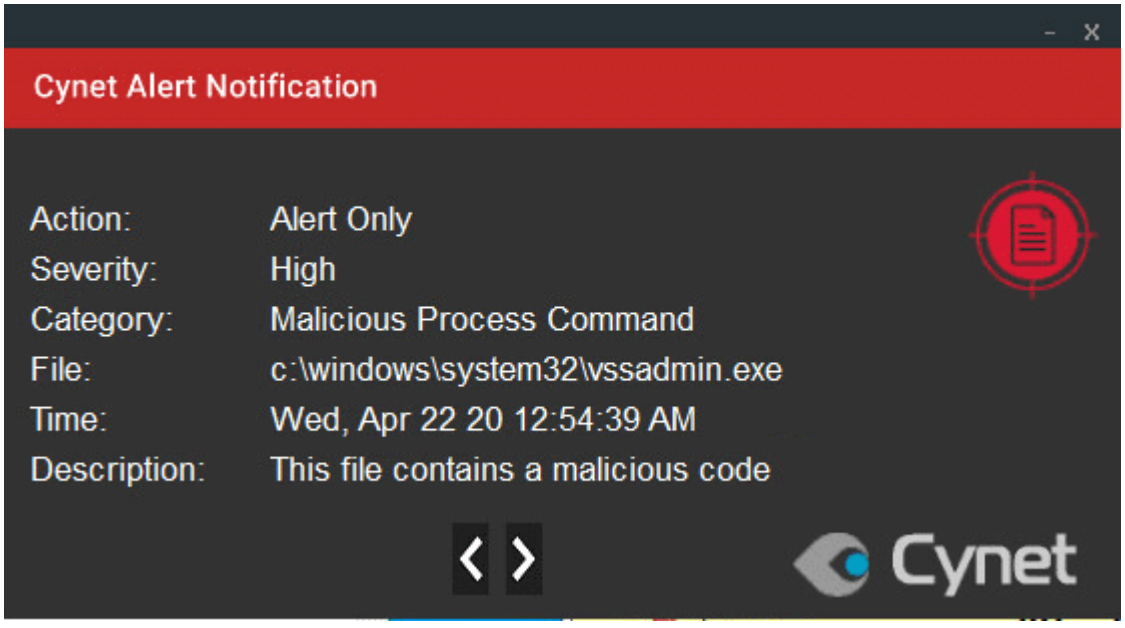
Attackers first began using the Ragnar Locker ransomware towards the end of December 2019 as a way to attack compromised networks. Ragnar Locker is a ransomware that runs on Microsoft Windows. It specifically targets software commonly used by managed service providers to prevent their attack from being detected and stopped. It is aimed at English-speaking users.
When the attackers first compromise a network, they will perform reconnaissance and pre-deployment tasks before executing the ransomware.

CYNET DETECTION

Cynet protects your environment against this type of attack. This type of attack is detected by Cynet alerting you to the malicious activities, using the following mechanisms.

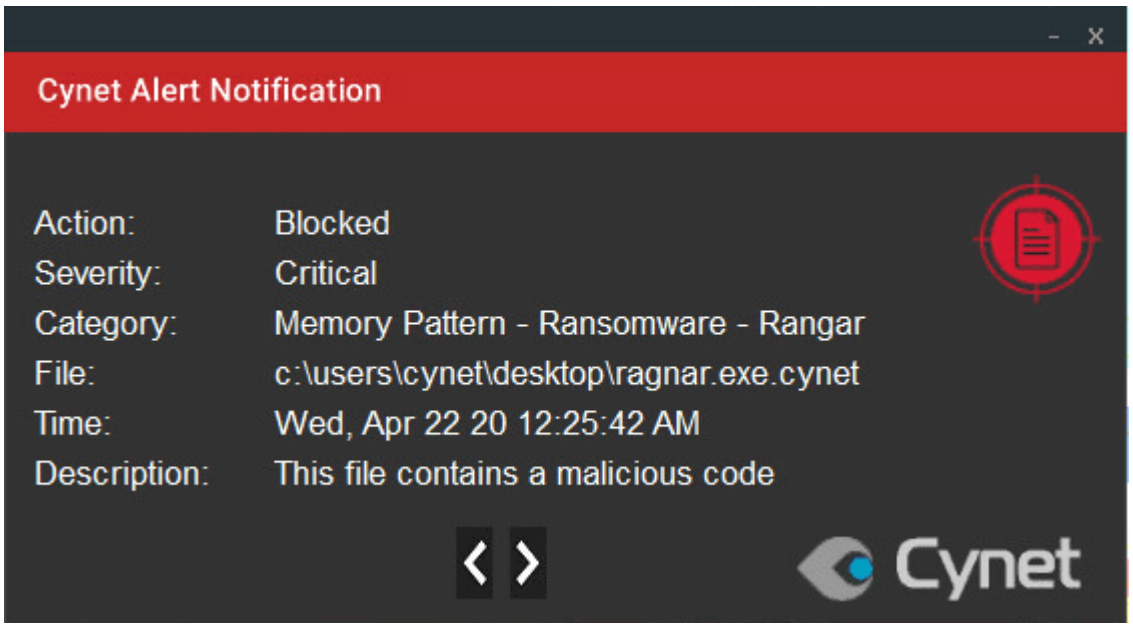
Note that some of the actions are set to alert only, to not interrupt the ransomware's flow, allowing Cynet to detect every step of Ragnar Locker Ransomware attack flow.

- **MALICIOUS BINARY**



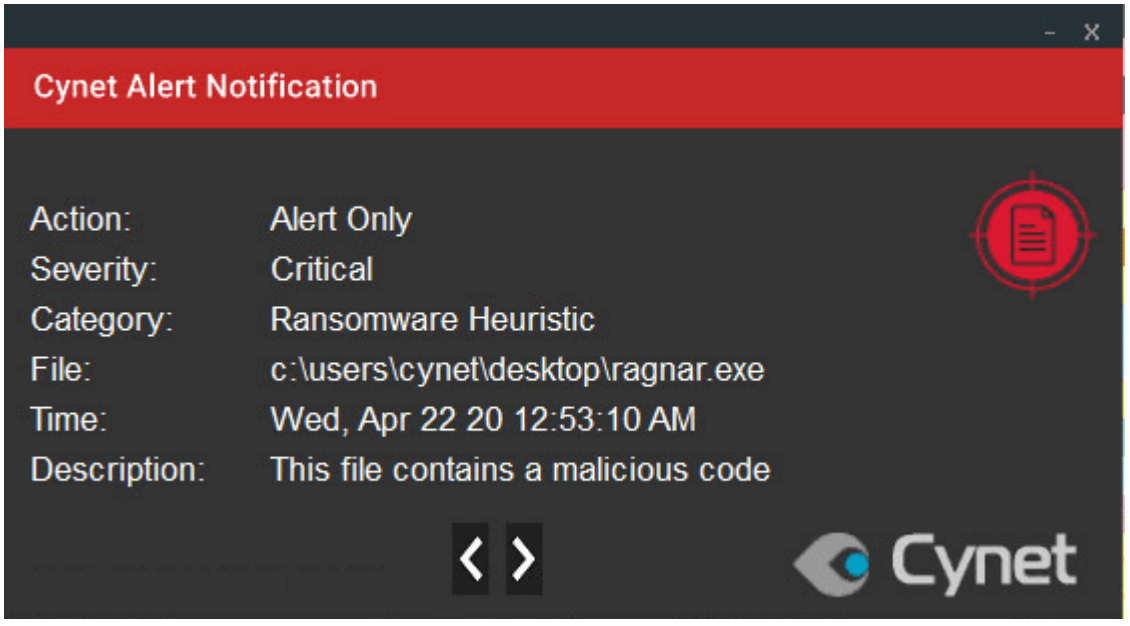
Fast Scan engine – This alert triggers when Cynet detects a file hash (SSDEEP) which is similar to a file hash that is flagged in our threat intelligence database as malicious. The idea behind this alert is to detect new variants of known malware.

- **MEMORY PATTERN**



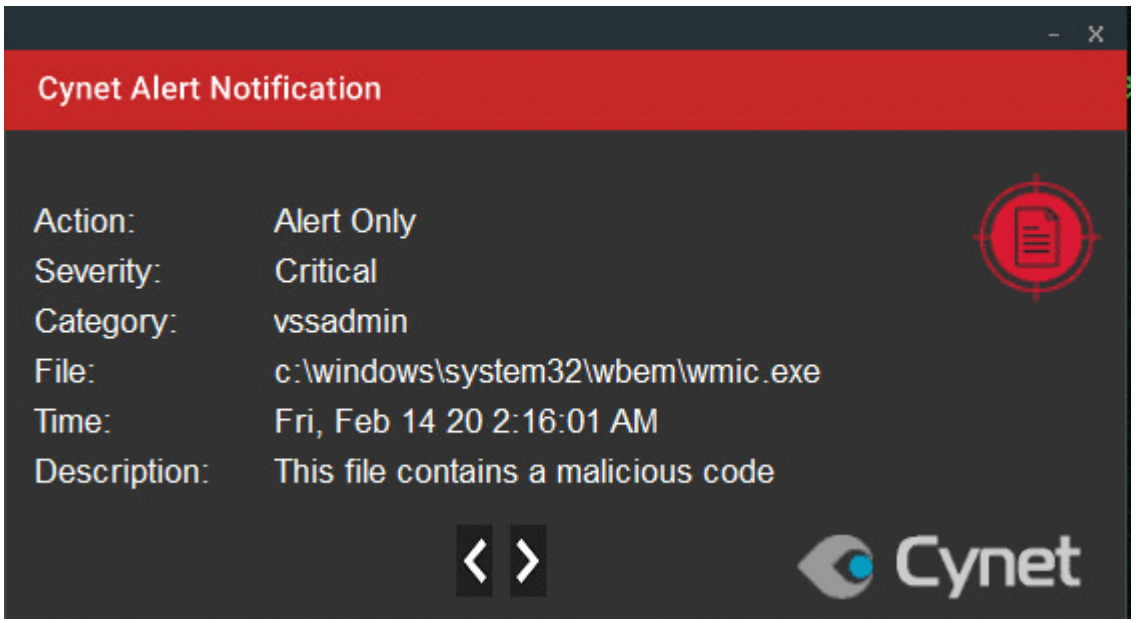
Default Configuration – This alert is triggered when Cynet detects memory strings which are associated with malware or with malicious files.

- **RANSOMWARE HEURISTIC**



ADT – Advanced Detection Technology – This alert triggers when Cynet detects suspicious behavior which can be associated with Ransomware (such as changing file extensions to ".Lock").

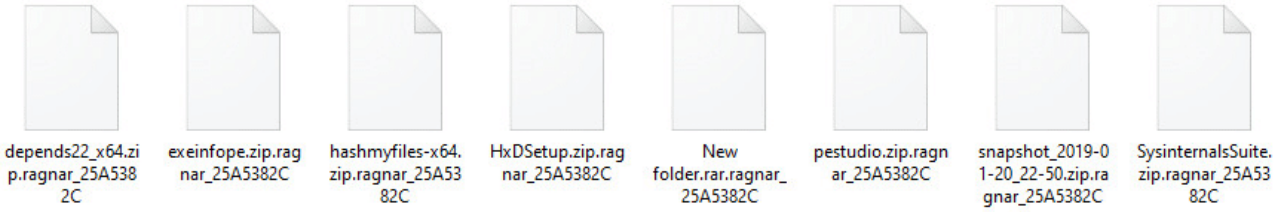
- **MALICIOUS PROCESS COMMAND**



ADT – Advanced Detection Technology – This alert triggers when Cynet detects a CMD process which executes a command that contains suspicious arguments or is associated with malicious patterns. "VSSADMIN delete shadow /all" is an approach of ransomware in order to delete the shadow copies. Shadow Copy is a technology included in Microsoft Windows that can create backup copies or snapshots of computer files or volumes, even when they are in use. It is implemented as a Windows service called the Volume Shadow Copy service.

INVESTIGATION OVERVIEW

After execution, Ragnar Locker Ransomware encrypts the files and adds the extension ".ragnar" and an 8 digit number:



When encrypting files, it will skip files in the following folders, file names, and extensions:

kernel32.dll	ProgramData	ntldr
Windows	All Users	ntuser.dat
Windows.old	autorun.inf	ntuser.dat.log
Tor browser	boot.ini	ntuser.ini
Internet Explorer	bootfont.bin	thumbs.db
Google	bootsect.bak	.sys

Opera	bootmgr	.dll
Opera Software	bootmgr.efi	.lnk
Mozilla	bootmgfw.efi	.msi
Mozilla Firefox	desktop.ini	.drv
$Recycle.Bin	iconcache.db	.exe

Once a computer's files have been encrypted and renamed, it creates a ransom note at several directories – the ransom notes are named RGNR_25A5382C.txt.

The note itself contains an email address to contact the cybercriminals who will provide a decryption tool once the victim sends them the Base64 code which also contains details of the infected host.


```
**********************************************************************************************************

 If you reading this message, then your network was PENETRATED and all of your files and data has been ENCRYPTED

                                          by RAGNAR_LOCKER !

**********************************************************************************************************

*********What happens with your system ?************

Your network was penetrated, all your files and backups was locked! So from now there is NO ONE CAN HELP YOU to get your files back, EXCEPT US.
You can google it, there is no CHANCES to decrypt data without our SECRET KEY.

But don't worry ! Your files are NOT DAMAGED or LOST, they are just MODIFIED. You can get it BACK as soon as you PAY.
We are looking only for MONEY, so there is no interest for us to steel or delete your information, it's just a BUSINESS $-)

HOWEVER you can damage your DATA by yourself if you try to DECRYPT by any other software, without OUR SPECIFIC ENCRYPTION KEY !!!

Also, all of your sensitive and private information were gathered and if you decide NOT to pay,
we will upload it for public view !

****

**********How to get back your files ?******

To decrypt all your files and data you have to pay for the encryption KEY :

BTC wallet for payment: 1E6EjTqYPHLj1uovPKKRXzMpPCcpAcVuiU
Amount to pay (in Bitcoin): 60

****

**********How much time you have to pay?**********

* You should get in contact with us within 2 days after you noticed the encryption to get a better price.

* The price would be increased by 100% (double price) after 14 Days if there is no contact made.

* The key would be completely erased in 21 day if there is no contact made or no deal made.
Some sensetive information stolen from the file servers would be uploaded in public or to re-seller.

****

**********What if files can't be restored ?******

To prove that we really can decrypt your data, we will decrypt one of your locked files !
Just send it to us and you will get it back FOR FREE.
```

RECOMMENDATIONS

- Use Cynet built-in remediation to isolate the host from the network.
- Delete all malicious payload associated with the Ransomware (rangar.exe).
- Use Cynet built-in remediation to prevent the malicious payload from running.
- Use Cynet Forensics to investigate the root-cause of this incident.

Contact Cynet CyOps (Cynet Security Operations Center)

The Cynet CyOps team is available to clients 24/7 for assistance with any issues, questions, or comments related to Cynet 360. For additional information, you may contact us directly at:

Phone (US): +1-347-474-0048

Phone (EU): +44-203-290-9051

Phone (IL): +972-72-336-9736

CyOps Email: soc@cynet.com
