Ministry of Government and Consumer Services

Ontario

TLP:WHITE

MEDIUM (Share within 24 hrs) Distribution Urgency

March 11, 2022

Cyber Security Advisory – Ragnar Locker Ransomware

Executive Summary

You are receiving this advisory to make you aware of some new intelligence on the Ragnar locker ransomware group.

Recipients of this information are advised to act and take precautionary measures to protect your organization's information assets, systems, and networks.

How does this affect my organization?

The Ragnar locker ransomware variant is one that exfiltrates data and operates a leak site where they attempt to name and shame victims into paying the ransom.

As a general best practice, it is strongly recommended that you use network segmentation, keep software up to date, use multi factor authentication and follow best practices.

What should I do?

As soon as possible, forward this notification to your cyber security personnel or IT partners for immediate action.

Technical Details

This ransomware is distributed through multiple vectors including exploits for unpatched software, RDP brute forcing and phishing emails.

The malware is known to do the following:

- Use existing Windows tools and utilities to manipulate and disable system recovery options, backups, and Volume Shadow Copies.
- Some versions of the ransomware have been known to target security products or processes which might interfere with the encryption process.
- To utilize the creation of a new Windows service, as well as the use of scheduled tasks for persistence.

The threat actor is known to terminate remote management software (such as Kaseya) used by managed service providers to remotely manage enterprise endpoint systems.

The threat actor is known to use off the shelf software for propagation and delivery including Mimikatz and PsExec, as well as RDP for lateral movement.

The actor is also known to use tools like Cobalt Strike and Metasploit.

The threat actor has been known to compress files and may download a file compression utility like Winrar or 7Zip and is known to use the Mega cloud storage site, as well as other publicly available file sharing services.

The threat actor operates a leak site where victim organizations data is leaked.

Recommended Action

- Ensure that you are using up to date antivirus.
- Ensure available patches are being applied in a timely manner across your infrastructure, especially the ones identified in this advisory.
- Ensure that you are following email best practices and your users are familiar with phishing and how to spot phishing messages. Review 5 Ways to Spot a Phishing Email.
- Ensure that access to RDP and other vulnerable services is disabled, if not required. Ensure that RDP is not directly exposed to the Internet for any system.
- Ensure that you have working and recent back ups.
- Enable multi-factor authentication, Including on VPN services, where possible.

- Review the enclosed tip sheet *What is Ransomware and How to Prevent Ransomware Attacks*.

In addition, please also consider the following:

- Drafting a Cyber incident response plan.
- Ensure your anti-malware software / endpoint protection scans your email messages.
- Do Google or Microsoft host your email? Check out the links below for information on enhancing security for G Suite and Office365.
    - G Suite Admin -Advanced Phishing and Malware Protection
    - Protect Against Threats in Office365

The identified indicators of compromise (IoCs) are listed below:

193[.]111[.]153[.]24
23[.]106[.]122[.]192
45[.]146[.]164[.]193
79[.]141[.]160[.]43
108[.]26[.]193[.]165
108[.]56[.]142[.]135
116[.]203[.]132[.]32
142[.]44[.]236[.]38
149[.]28[.]200[.]140
162[.]55[.]38[.]44
185[.]138[.]164[.]18
185[.]172[.]129[.]215
190[.]211[.]254[.]181
193[.]42[.]36[.]53
193[.]42[.]39[.]10
198[.]12[.]127[.]199
198[.]12[.]81[.]56
217[.]25[.]93[.]106
23[.]227[.]202[.]72

37[.]120[.]238[.]107
45[.]144[.]29[.]2
45[.]63[.]89[.]250
45[.]90[.]59[.]131
45[.]91[.]93[.]75
47[.]35[.]60[.]92
49[.]12[.]212[.]231
5[.]45[.]65[.]52
50[.]201[.]185[.]11
89[.]40[.]10[.]25
95[.]216[.]196[.]181
prod12ms[.]com
ssl-secure-com2048[.]com
vivopsalrozor@yahoo.com
titan_fall572cool@gmail.com
shingxuan7110@protonmail.com
sh0d44n@gmail.com
scanjikoon@yahoo.com
michael.shawn.brown2@gmail.com
gamarjoba@mail.com
back.shadow98@gmail.com
alexeyberdin437@gmail.com
alexeyberdin38@gmail.com
alexeyberdin17@gmail.com
alexeyberbi@gmail.com
alexey_berdin@list.ru
151Ls8urp6e2D1oXjEQAkvqogSn3TS8pp6
19kcqKevFZhiX7NFLa5wAw4JBjWLcpwp3e
1CG8RAqNaJCrmEdVLK7mm2mTuuK28dkzCU
izugz[.]envisting[.]xyz

More information:

- FBI Flash - CU-000163-MW

For Further Information

If you find any of the indicators of compromise (IOCs) on your networks, or have related information or any questions, please contact cyberadvice@ontario.ca.

The Cyber Security Centre of Excellence has a learning portal that provides IT & security professionals and change management leaders in the Ontario broader public sector with foundational learning on cyber security. The Cyber Security Ontario Learning Portal is administered by the Cyber Security Centre of Excellence within the Cyber Security Division of the Ontario Ministry of Government and Consumer Services.

To learn how the Cyber Security Centre of Excellence strengthens cyber security in the broader public sector, visit Cyber Security Centre of Excellence.

No Warranty

This Cyber Security Advisory may contain third party content and links. The Cyber Security Centre of Excellence does not control or maintain third party links and makes no representation or warranty that the link: (a) will still work when you click on it; or (b) will deliver service or content that is useful, appropriate, virus-free or reliable. It is your responsibility to determine whether to access a link or agree to receive or rely on any service or content that is made available to you.

The Cyber Security Centre of Excellence is providing information about a known threat for potential use at the sole discretion of recipients to protect against cyber threats. This notification is provided to help broader public sector organizations enable cyber preparedness and resilience.

Definitions

Cyber Security Threats or Incidents are events that may present risk to the security (i.e. confidentiality, availability or integrity) of an organization's information assets, systems and networks.

- Cyber Security **Threat** Advice is issued when **no active exploits** are observed. The purpose of threat advice is to enable organizations to prepare for and mitigate cyber threats.

- Cyber Security **Incident** Advice is issued when an **active exploit** is observed. This information is time sensitive. The purpose of incident advice is to inform organizations of an ongoing cyber incident so the organization may prepare for timely response and remediation.

Cyber Security Centre of Excellence uses the traffic light protocol (TLP) for the sharing of information with parties external to the government of Ontario with public program information with TLP:WHITE; and non-public program information with TLP:GREEN.