Conti Ransomware Victim Questionnaire

The following questionnaire will assist the FBI and your organization in determining if you are a victim of Conti Ransomware and may help mitigate the threat of further infection.

Brief Synopsis: The FBI opened an investigation into the Conti Ransomware in the summer of 2020. To date there are over 150 victims world-wide attributed to Conti. The ransoms vary widely and appear to the tailored to the victim. Victims are instructed to reach the subjects through an online portal. If no ransom is paid the victim's data is published to a shame site or sold.

RAAS Model:

- We are not seeing consistency across victim which is attributed to the utilization of multiple affiliates
- Please gather as much information about the attack to determine which affiliate is responsible for the intrusion
- The affiliates always exfiltrate data for later extortion or sale
- The subjects will negotiate ransom amounts with the victims
- The affiliates will maintain access to the network after the initial attack unless the network is cleaned
    - Affiliates will resell future access
    - Affiliates will re-encrypt the network if attempts are made to re-constitute

Tools:

- Cobalt Strike
- Mimikatz
- Powershell
- Trickbot Bazarloader
- rclone
- Anchor DNS

Questions

The Compromise:

- What was the date and time of the incident?
- Did the encryption event take place over a weekend?
    - Overnight during the week?
    - In response to some sort of IT security action?
- How many systems are encrypted?
    - What type of systems?

Impact:

- What is the impact to operations?
    - Is the organization able to operate?
- What is the estimated monetary loss to the organization?
    - Overtime?
    - New hardware/software?
    - Outside assistance?
- Who from the organization is handling the incident?
    - Who should be the POC?
- How is the organization handling remediation?
- Was a remediation company contacted? If so;
    - What was the company?
        - Is there a POC?
    - Did the remediation company provide a report?
        - Can we get a copy?
    - Did the remediation company make forensic images?
        - If so, can we get a copy?
- Was victim data confirmed to be posted to the Conti leak site?
    - Was data removed from site if ransom was paid?
    - Did Conti actors provide a list of files stolen?
        - Did the files provided by Conti match what was on the leak site?
        - Where were the files stolen from?

Ransom Payment:

- Does the organization have a copy of the ransom note?
- Was the note in a text file?
    - What was the file name of the text file?
- Can that file be collected or the information from that file be collected?
- Is the organization still in contact with the actor(s)?
- To your knowledge, have the actor(s) contacted any other organizations concerning your encryption event in an attempt to further intimidate you?

Otherwise:

- What accounts were used by the actor(s)?
    - Website?
    - Email?
        - IP address or header information?
    - Other Communication Method?

- Did the organization contact the actor(s)?
    - Did a third party? If so, who?
- How did the actor(s) request to be contacted?
    - Tor?
        - If yes, please provide address
    - Email?
        - If yes, please provide address
- Cryptocurrency
    - Subject cryptocurrency wallet
    - Victim cryptocurrency wallet
    - Victim IP address
- Was the ransom paid?
- How much ransom was paid?
- When was the payment made?
- Was the decryptor provided?
- How was the decryptor provided?
    - If via website, what website?
    - If via email, what email?
- Did the decryptor work?
- Did the victim converse with the subject about how the compromise occurred?

Forensics/Mitigation:

Besides any possible images collected by the remediation company:

- Are any encrypted machines still running since the time of the event? Can we obtain memory images? If a Virtual Machine (VM) was used, can we have the VM suspended and virtual memory files captured?
- Are any encrypted machines, or backups/images of encrypted machines still within control of the organization? Can we obtain disk images? If VM, can we get clones?
- In order of precedence, machines which we would ideally like images/backups/clones of are the following:
    - Identified patient zero machine
    - Presumed possible patient zero machine
    - Domain controllers
    - Terminal Server/RDP Server
    - Active Directory servers
    - Email Server
    - Backup Server

Did the organization see a spike in phishing emails prior to the encryption event?

- Are there email server/system logs available for the weeks leading up to encryption?
- Were there emails with macro-enabled word or pdf documents? Can we obtain a copy?
- Were there emails impersonating government agencies or well-known security vendors? Can we obtain copies of the emails with full headers?

Did the organization observe any users visiting fake cryptocurrency exchange websites prior to the encryption event?

- Are there any client-side web access logs that show access visited the fake cryptocurrency exchanges?

Does the organization have a basic network diagram available? Can we obtain a copy?

What are the organization's public facing IP addresses?

Was there any evidence of data exfiltration or an unexpected spike in network traffic bandwidth usage?

Does the organization have any log files available from the weeks prior to the encryption event? Logs sought include:

- Firewall logs
- Email server or service logs
- Net flow
- Windows security event logs
- AV logs

Has the organization identified the ransomware executable itself? For each instance found, please provide the following:

- Executable File Name
- Description of the machine and or server i.e. Windows server or PC workstation
- File path/location
- Annotate if a copy can be provided

Does the organization have a timeline of events to include any uptick in virus notifications, phishing emails, abnormal behavior, before, during or after the encryption event?

Does the organization use tools such as Powershell, psExec, RDP, batch files, etc… to administer the network? If so, with what frequency or in what capacity?

Did the organization do some sort of security update/virus cleanup/password reset/etc… activity just before the encryption event? Were they making plans to do it as the encryption event took place?