10 Ways Symantec Incident Response Can Help with Ransomware

Ransomware forces its victims – individuals and organizations – to pay ransom through specifically noted payment methods in order to grant access to their machine, or to get their data back.

The growth of these types of ransomware attacks is accelerating, as seen with recent high profile attacks. It's important to understand your options should you fall victim**. Symantec Incident Response** can help organizations both to validate an attack and to make decisions on what to do next.

In this document, you'll find 10 ways **Symantec Incident Response Services**, part of Symantec **Cyber Security Services** that also include **Managed Security Services** for Monitoring and **DeepSight Intelligence** Services, uses **Symantec Security Analytics, formerly BlueCoat Security Analytics Platform,** to help organizations right now, depending on their situation, that are infected with ransomware.

1. **We can help identify the primary infector and contain further spread.**

   More info: Our research and past engagements have discovered that ransomware is rarely the primary infector. Either a SPAM email with malicious hyperlink/file attachment, Drive---by---Downloads / Watering Hole Attacks, Malicious Downloaders / Droppers, or other malware e.g. Trojan.Zbot are responsible for an initial infection that then leads to a follow-on ransomware attack.

   Using **Symantec Security Analytics, formerly BlueCoat Security Analytics** network forensic platform, we can analyze malicious traffic to identify additional active attacks that may be going undetected within your environment. This holistic approach to the incident ensures that we identify the primary attack vector, which is critical to understanding the attacker's primary campaign target, and ensures that you aren't missing the actual attack by focusing solely on the ransomware activity.

   Our **Incident Response Services** can then take appropriate steps to engage the adversary, contain the attacks, and work to recommend ways to prevent the primary infector in the future.

> ***Fast Fact***
>
> *"In 2016, the average ransom spiked 266 percent with criminals demanding an average of $1,077 per victim."*
>
> *2017 Symantec Internet Security Threat Report*

2. **We can provide incident-specific recommendations to prevent success of future similar attacks.**

   Use case exhibiting points 1 & 2: Symantec Incident Response was contacted to assist in a ransomware infection. The malware was encrypting PDF and executable files on network shares and exhibiting network worm-like behavior. The customer was experiencing the outbreak in two global centers, causing significant disruption to their environment.

   Using **Symantec's Endpoint Protection** and **Symantec Security Analytics, formerly BlueCoat Security Analytics** products, **the Incident Response Services** team confirmed a new malware variant was being utilized. The malicious code was identified on a number of endpoints and numerous file shares within the organization. Symantec Incident Response was able to contain and eradicate the threat.

   By performing an in-depth analysis of all data available, **Symantec Incident Response** was able to identify the

cause of the repeated infections and assist the customer with implementing controls to prevent any further outbreaks as well as assisting them to enhance their endpoint protection environment overall. Within 72 hours the environment was under control, which included Symantec's identification and removal of multiple additional threats including undetected banking Trojans.

The Incident Response team coordinated with **Symantec Managed Security Services** and **DeepSight Intelligence** teams throughout the engagement to provide quicker remediation. Malware Reverse Engineers wrote a decryption tool that was able to decrypt infected PDF files infected with this particular malware.

3. **We can identify Patient Zero.**

More info: Patient Zero is the root cause of a ransomware attack. By identifying this person or system, you're able to determine the level of administration privileges the attacker may have gained access to and better determine the trajectory of the attack after the initial compromise.

Determining Patient Zero requires a broad view of the environment to reconstruct the spread of the attack. **Symantec Incident Response** teams have network and endpoint forensics products at their disposal, powered by the Symantec Global Intelligence Network, to quickly and accurately understand the attack's chain of events.

4. **We can determine whether the victim organization is the primary target or merely collateral damage to gauge risk of reinfection.**

> ***Fast Fact***
>
> *"Ransomware continued to escalate as a global problem in 2016. Symantec identified a 36 percent increase in ransomware attacks worldwide."*
>
> *2017 Symantec Internet Security Threat Report*

Use case: During an incident investigation, Symantec's investigators have access to Symantec's Global Intelligence Network, including threat and adversary intelligence from **DeepSight Managed Adversary and Threat Intelligence**, and telemetry on hundreds of millions of endpoints and millions of attack sensors. With this information, **Symantec Incident Response Services** can determine how widespread the attack is, who the attackers are, the attackers' level of sophistication, whether or not other variants of the attack exist, and any Indicators of Compromise (IOCs) related to them. This intelligence combined with findings from using **Symantec Security Analytics, formerly BlueCoat Security Analytics** platform, allows **Symantec Incident Response Services** investigators to develop more robust containment plans and make better remediation recommendations to prevent further attacks of the same type.

Additionally, we regularly see customers taking the approach of wiping an endpoint effected by ransomware and putting it back into circulation without a second thought. In one scenario, the attackers used wiper tools to cover their tracks after conducting a targeted, multi-stage attack across the customer environment. Had that customer not engaged us to investigate the ransomware issue, the attackers would most likely still be in their network.

This validates Symantec's stance on advising victims not to pay the attackers for the following reasons:

- Paying the ransom puts you on the future target list of attackers who want to maximize their hit rates. As a former payer, you are more likely to be targeted a second time.
- Paying attackers only perpetuates the problem and keeps the incentive for these attacks going.

10 Ways Symantec Incident Response Can Help with Ransomware

5. **We can determine if ransomware is actually encrypting data or deleting and overwriting data.**

   Use case: In the use case above, we were able to determine that the data had, in fact, not been encrypted. The attackers had planted ransomware notices to give the customer the impression that the data was encrypted in an attempt to masquerade their true intentions.

   This validates Symantec's stance on advising victims not to pay the attackers for the following reasons:

   There is no guarantee the files are actually encrypted. In our ransomware investigations we have seen cases where the data is not actually encrypted. Engaging **Symantec Incident Response** Services in a ransomware incident can lead to a more informed decision by the customer on what steps to take next.

6. **We can help victims create a data recovery plan by analyzing the malware to determine how data was encrypted.**

   Use case: Ransomware denies access to a user's data by encrypting it and deleting the original copy. The methods in which ransomware accomplishes these tasks varies widely in terms of sophistication. In the worst case, the malware implements the cryptographic algorithm correctly, exercises proper key management, and securely deletes the original copy of the user's data. In many cases, however, the malware writer makes mistakes in implementation that can be exploited by incident responders to recover data more easily. A skilled malware analyst can reverse engineer the ransomware to identify any weaknesses in implementation and help the user recover their data.

> ***Fast Fact***
>
> *"There's evidence that ransomware attackers have begun tailoring their ransom demands on the basis of the type and volume of data they have encrypted."*
>
> *2017 Symantec Internet Security Threat Report*

7. **We can work with the customer's data recovery provider to help determine their best plan of action based on the specific threat.**

   Use case: In many cases, customers hire a data recovery service to assist in the ransomware recovery process. The recovery process is unique to each individual situation and can depend heavily on the sophistication of the malware used. After analyzing the malware to understand how it encrypts and erases data, Symantec Incident Response Services can work with the data recovery provider to develop an efficient and effective data recovery plan.

8. **Incident Response Services is truly a team sport. In the role of Breach Coach, we help customers in decisions regarding both internal and external communications, reporting requirements, interaction with Law Enforcement, etc.**

   More info: Many customers overlook the non-technical aspects of a ransomware attack, which can have an equal or greater impact on a business that the technical aspects of an attack. Symantec Incident Response Services investigators have, on average, a decade of experience handling a wide variety of cyber attacks and can assist our customers in understanding the non-technical aspects of an attack and helping them make smart decisions.

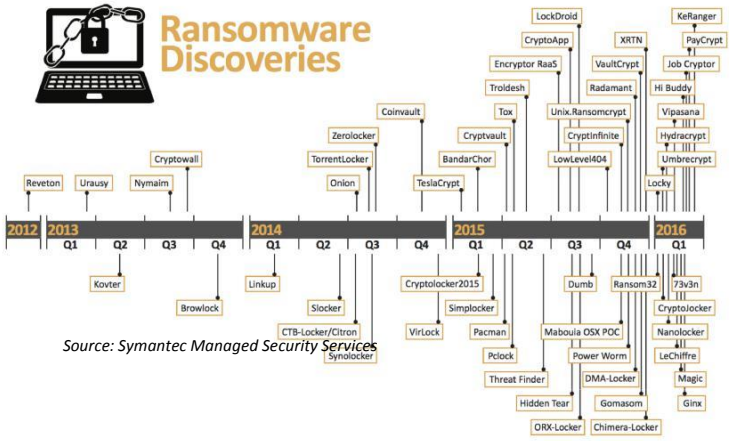
10 Ways Symantec Incident Response Can Help with Ransomware

9. **Through our relationship with DeepSight's Managed Adversary and Threat Intelligence (MATI) team, we are able to provide additional intelligence about the attackers, providing customers with more context around the incident.**

   More info: Assigning accurate attribution and determining motives will aid greatly in preventing future attacks. For example, if an incident response team is able to determine that the adversary in a specific attack is a nation-state, you're able to take a look at the other tactics commonly seen in that particular nation and raise your defenses in those areas in an attempt to thwart future incidents from happening.

10. **We can help customers understand how to protect themselves from future attacks.**

    Use case: In one scenario, a customer had been infected with Cryptolocker, and upon further investigation it was determined that the initial compromise resulted from a phishing attack. Understanding that there was a weakness in the human layer of security helped the company prioritize better end user training and put in place a more thorough skills development program, strengthening their weak points.



Source: Symantec Managed Security Services

As seen in the chart to the right, it's clear that adversaries are getting creative when it comes to creating new types of ransomware. They're seeing its effectiveness and taking full advantage. With help from **Symantec Incident Response**, ransomware doesn't always have to equal disaster.

For more information on Symantec Cyber Security Services, visit:
https://www.symantec.com/services/cyber-security-services

If you need help with a security incident right now, please contact us.

Email: incidentresponse@symantec.com
US Incident Response Hotline: (855) 378-0073
UK Incident Response Hotline: +44 (0) 800 917 2793