Accelerated Response to Ransomware Targeting Educational Institutions

Using Cisco Stealthwatch Network and Cloud Security Analytics

Cyber criminals have always had an eye on educational institutions as they are considered easy or weak targets due to the lack of IT resources and budget dedicated to security. Also, the nature of the sensitive data and the reliance on the computing systems for day-to-day functioning makes any disruption highly critical. And attackers are exploiting this through ransomware threats, that have become more frequent in the recent years.

Cybersecurity experts recommend backing up data. In the event of a ransomware attack, when a school's access to their system is blocked, they can recover their systems using the back-up. It is also recommended to not agree to pay the ransom (exceptions for isolated incidents), as this will motivate the adversaries even further.

The reality of today's attack landscape: attacks are inevitable

You can deploy multiple layers of preventive security, but the attackers are persistent, have unlimited resources at their disposal and need to be right just once. Thus, 100% ransomware prevention might not be attainable. Institutions should also have an effective tool in place to investigate and respond to the ransomware incident. Cisco Stealthwatch is a security analytics solution that collects and analyzes data from every part of the network, and alerts on suspicious behavior. Using a combination of behavioral modeling, machine learning and global threat intelligence, Stealthwatch can quickly and with high confidence, detect threats such as C&C attacks, ransomware, DDoS attacks, illicit cryptomining, unknown malware, as well as insider threats. With a single, agentless solution, you get comprehensive threat monitoring across the data center, branch, endpoint and cloud, and even encrypted traffic.

Stealthwatch helps organizations stay ahead of ransomware and other security attacks.

- Detect threats early by pinpointing suspicious behavior
- Correlate local threats to global campaigns
- Perform forensic analysis for incident response

"Stealthwatch was able to catch Emotet within our environment. We were able to quickly determine what machine was infected and prevented it from spreading.

The executable was too new to have a malicious disposition, and was also packaged and delivered in a way that allowed it to bypass all our other security tools. Only Stealthwatch caught it."

Don Bryant
Chief Information Security Officer,
University of North Carolina (UNC) Pembroke

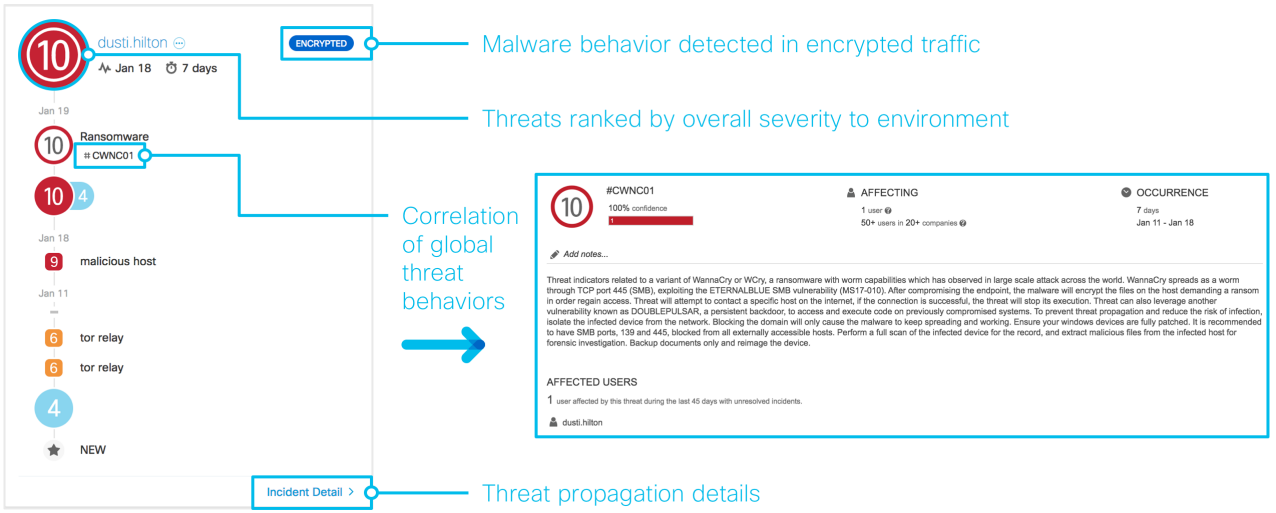
Here's how Stealthwatch can specifically help respond to a ransomware attack:

Detect threats early by pinpointing suspicious behavior

Ransomware attacks are generally initiated through methods like a phishing email or exploitation of a vulnerability. It might involve behavior such as port scanning, command-and-control (C&C) communication back to the attacker network, etc. Whatever means the attackers use, the activity touches the network, and that's where Stealthwatch comes in. It's constantly collecting and analyzing the entire network traffic, looking for suspicious behavior and will immediately alert on it. Additionally, you can create custom security policy alerts within Stealthwatch to detect restricted communications such as use of SMB protocol, or access to sensitive data servers from outside the network.

Correlate local threats to global campaigns

Stealthwatch uses the power of multi layered machine learning to process billions of network sessions to determine all the malicious domains and servers across the world. It is combined with threat intelligence from Cisco Talos, which is the largest non-government threat organization in the world, to discover all the global campaigns. Using this information, Stealthwatch can correlate any communication happening within your institution to a malicious network as part of either a known global campaign, or an unknown targeted attack. Also, using Encrypted Traffic Analytics, Stealthwatch can detect threats in encrypted traffic, without any decryption.



Stealthwatch can detect ransomware hiding in encrypted traffic, and can also correlate it to global campaigns like WannaCry here

“Locating devices and verifying attacks used to take us days and this has been *cut to a few minutes.*

We are now aware of some attacks that used to go undetected.”

Network Engineer
Educational Institution

To learn more about Stealthwatch, go to: https://www.cisco.com/go/stealthwatch

Find what threats are lurking within your network by signing up for our free visibility assessment at: https://cisco.com/go/stealthwatch-free-assessment

1956036 10/2019

Perform forensic analysis for incident response

Stealthwatch has the ability to store telemetry for long periods of time. If you are impacted by a ransomware attack, the incident response team needs the contextual information to answer questions like – What was the source of the threat? What systems were infected? How did they get in? Are the attackers still in the network? – and more. With Stealthwatch, you can go back to a certain period of time and analyze flows in-depth. Also, each alert within Stealthwatch is associated with an entity connected to the network, and you can also view all the communications occurring to and from that entity laterally within the network or externally. All this results in a quick and effective response and exposes root-cause to prevent future attacks.

Flexible deployment options

Stealthwatch offers different deployment models: on-premises as a hardware appliance or a virtual machine - Stealthwatch Enterprise. Or cloud-delivered as a SaaS solution – Stealthwatch Cloud. For educational institutions with lean security teams, the SaaS-based Stealthwatch Cloud is a great option as it’s easy to deploy and simple to consume. Get started on the free 60-day trial of Stealthwatch Cloud today.