Defending Against Ransomware With Zscaler™ Workload Segmentation

Securing east-west application communications and stopping lateral movement of threats

Harry Sverdlove
Chief Technologist, Secure Workload Communication, Zscaler

Contents

Introduction: U.S. Healthcare Being Held Hostage (Again)

In 2020, the world faced one crisis after another, and the cybersecurity world was no exception. The Cybersecurity and Infrastructure Agency (CISA), Federal Bureau of Investigation (FBI), and HHS (Health and Human Services (HHS) issued a warning last week that the public health sector was facing an increased threat from a ransomware campaign. Several hospitals in the United States had already been targeted.

Such attacks are not new. In 2019, there were more than 140 ransomware attacks against governmental and health care organizations. Ransomware attacks have become increasingly common, sophisticated, and effective over the past decade.

To summarize, ransomware is a type of attack in which critical files or an entire operating system is encrypted without the user's knowledge, rendering the system unusable until the victim (or victim's organization) pays a ransom (typically in cryptocurrency) to obtain the decryption key. In other words, ransomware is a financially motivated attack carried out by cybercriminal organizations. On rare occasions, this style of attack is done solely to disrupt a target's infrastructure, but more generally, it is driven by the desire to profit via ransom payments.

How Does Ransomware Work?

For ransomware to be effective, it has to impact as many systems as possible within a network. For example, if only one system were encrypted and disabled out of thousands of systems, the victim is more likely to just unplug and rebuild that one system. The more systems or files impacted, the more likely the victim will be inclined to pay the ransom. While law enforcement officials and cybersecurity experts recommend that you *never* pay a ransom, the reality is that when a business is losing millions of dollars a day in downtime and is facing the potential of weeks or months to manually recover, the temptation to resolve the issue with an expedient payment is understandable.

In this current campaign, a phishing email is sent to individuals associated with a target organization. The email either contains a piece of malware (as attachment) or links to a

compromised website that can deliver the initial malware payload. The initial malware belongs to the TrickBot (and its associated BazarLoader/BazarBackdoor trojans) family.

TrickBot is then capable of installing itself surreptitiously into various Windows processes, establishing a backdoor to a command-and0-control (C&C) server, downloading additional components, using common tools to map out the network, and finally propagating throughout that network. TrickBot has specific modules that can propagate to domain controllers via an SMB exploit or via Remote Desktop Protocol (RDP).

As TrickBot spreads, each infected computer downloads and launches the Ryuk (or its successor Conti) ransomware which is capable of encrypting both local and shared network files.

The ransomware script is always the same:

1. Trick a user into downloading and executing a malicious loader file (or use an exploit to do this without the user's knowledge)
2. Have the loader file contact a server (or other compromised systems) to download more components
3. Surveil the network to identify other systems and file shares
4. Spread to as many systems as you can, especially critical infrastructure like domain controllers
5. Encrypt files to disable the system(s) entirely or prevent access to specific data

There can be variations on the details, as well as lots of additional obfuscation and destruction that can be deployed, but the playbook is still the same.

How To Stop Ransomware

Most security recommendations involve addressing steps 1 and 5 above in the attack sequence. For step 1, it is recommended that you use email filtering and user education to prevent users from clicking on suspicious downloads or web links. While a good idea, this is obviously and woefully inadequate, otherwise ransomware attacks would not continue to rise in frequency. Attackers have become more sophisticated and it is becoming increasingly hard to distinguish malicious emails

from legitimate ones. Moreover, there are other ways to trick users, such as compromising websites that targeted users may frequently visit (a practice known as waterholing).

For step 5, the recommendation is to have a robust backup and recovery plan, so you can easily wipe and restore a system should it become compromised and encrypted. This is a good recommendation because it also helps in disaster recovery scenarios. But (a) ransomware is becoming more sophisticated and can target your backup copies as well, and (b) have you ever tried to restore just a single system let alone a domain controller or hundreds of systems across an organization? It's not only a nightmare, but it can take weeks and some data will inevitably be lost.

Zscaler Workload Segmentation focuses on steps 2 through 4. If the malicious payload cannot contact its C&C server or is unable to surveil the network or propagate to other systems, the attack can be thwarted in its tracks, or at least minimized in scope.

This is where a zero trust approach to east-west traffic is most effective. Zero trust means only authorized entities, such as applications, users, and devices, are able to communicate with other authorized entities. The assumption is that the network itself, and its addresses/ports/protocols, are inherently insecure. Trust is established by "who" is communicating, not just by "how" they are communicating.

Most networks are overly permissive when it comes to allowing systems within the same network to communicate with each other. At least 87 percent of allowed pathways within most corporate networks are either not used or not needed. This over-permissiveness exists because traditional firewalls do not provide the granularity needed to actually restrict traffic based on the entities using those connections. For example, let's say you are using Active Directory, and you need your domain controllers and clients to communicate on ports 88 and 135. With a traditional firewall, the best you might be able to achieve is restricting traffic based on your network IP addresses and those ports. Any malicious piece of code can still use those same addresses and ports to communicate with the controller for information-gathering purposes or even exploitation.

NGFWs, or next-gen firewalls, are capable of inspecting the traffic to see if it conforms to expectations, but malicious software can easily bypass this by simply using syntax that the NGFW considers "legitimate." Moreover, the connection has to actually occur for the NGFW to identify

anything suspect, and in some exploits, by the time the connection is identified as “bad,” the damage has already been done. In addition, deploying NGFWs to every choke point between every system can be prohibitively expensive and introduce significant network lag—whether we are talking about physical networks or virtualized cloud environments.

Zscaler Workload Segmentation (ZWS) takes a different approach to microsegmentation. It provides network security based on the true identity of the applications and services communicating. Unauthorized or malicious software is prevented from communicating, even if it is using the very same addresses, ports, and protocols allowed by a traditional firewall, and even if it is using the very same syntax identified by packet inspection within an NGFW.

There are many other advantages to using identity-based microsegmentation within your network, including easier deployment (no infrastructure changed required), policy compression and easier management (substantially fewer policies required), auto-scaling policies (because policies are based on identity not network addresses), and better visibility into your network (understanding how applications communicate, not just addresses). From a strictly security standpoint, the identity-based security of ZWS could have easily prevented a malicious loader from downloading additional components, from using even legitimate software already on the system to surveil and catalog the network, and from propagating to other systems using techniques such as RDP or PSEXEC.

Stop The Sequence, Stop The Attack

Educating users to defend against phishing attacks and having a backup strategy to recover in catastrophic cases are good strategies, but alone they are inadequate to stop ransomware. The majority of the stages of attack for ransomware involve unauthorized communications of malicious or compromised software. Traditional firewalls do not help, but ZWS identity-based segmentation will effectively stop ransomware from iterating and propagating through your environment. It’s time to stop being held hostage by ransomware.

Note: The Zscaler Threat Library and Cloud Sandbox will detect both Ryuk and Conti. Further technical details are available here.