AVERTIUM®

eBook

LEVERAGING ZERO TRUST ARCHITECTURE TO CONTAIN & COMBAT RANSOMWARE

hello@avertium.com

TABLE OF CONTENTS

Introduction ____ Page 2

ZTA Basics ____ Page 2

How Does Ransomware Work ____ Page 5

Recent Ransomware Attack Profiles ____ Page 8

Combating Ransomware with ZTA ____ Page 9

Avertium Customer Story ____ Page 9

Conclusions ____ Page 11

Avertium's Approach ____ Page 11

INTRODUCTION

What's keeping cybersecurity professionals up at night these days? **Ransomware.**

While ransomware is anything but new, its prevalence, as well as the cost of remediation, has grown tremendously in recent years. This is due to two reasons: Accessibility and Opportunity.

Accessibility

The rise of Ransomware-as-a-Service (RaaS) transforms a once-complicated, custom-coded malware campaign into a templatized package, removing barriers for novice cybercriminals looking to launch fairly sophisticated ransomware attacks.

Opportunity

The rise of remote working environments means more devices to monitor and less oversight, thus expanding the window of opportunity for bad actors.

The truth is, traditional, perimeter-based network security just doesn't cut it anymore... And this has given rise to Zero Trust Architecture (ZTA).

By shifting the network perimeter to wherever a user is located, ZTA works on a *"never trust, always verify"* premise, effectively shrinking down that window of opportunity for cybercriminals.

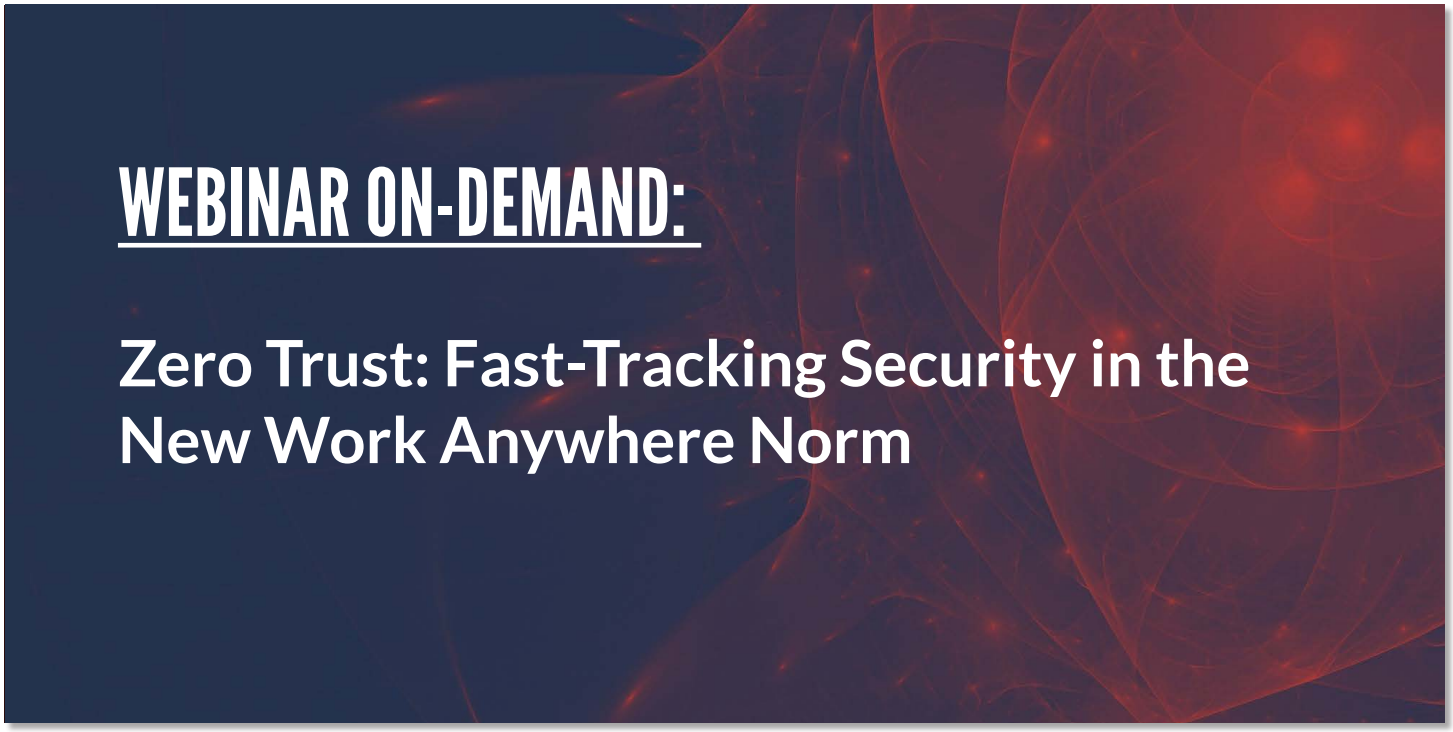
ZTA BASICS

It's systems and infrastructure-based.
For a baseline understanding, NIST defines Zero Trust Architecture (ZTA) as using zero trust principles to plan industrial and enterprise infrastructure and workflows. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned).

Authentication and authorization happen at both ends of the connection. Authentication and authorization (both subject and device) are discrete functions performed before a session and until an enterprise resource is established. Zero trust is a response to enterprise network trends that include remote users, bring your own device (BYOD), and cloud-based assets that are not located within an enterprise-owned network boundary.

Zero trust focuses on protecting resources - not network segments. Due to the diminishing relevance of the actual network boundary being the prime component to the security posture of enterprise resources, ZTA focuses on protecting things like assets, services, workflows, network accounts, etc.

To dive deeper, check out Avertium's on-demand webinar, "Zero Trust: Fast-Tracking Security in the New Work Anywhere Norm."



HOW DOES RANSOMWARE WORK?

A user's device (typically a PC/Server) is attacked from one vector or another and prevents them from accessing their resources by encryption methods. Another type of ransomware, Leakware or Extortionware, is where a thief will steal sensitive or damaging files and threaten to leak them publicly until the ransom is paid. In some types of businesses, the competitive edge is so important to have trade secrets exposed that it's just as damaging as having data encrypted.

The hacker then demands payment of one form or another for unlocking those resources. Once payment is made, attacker unlocks resources or destroys stolen files (in theory).

Some forms of ransomware can gain access to Mobile OS via SMS, but we will primarily be concerned with how it compromises a PC or Server asset in this paper. Ransomware, another type of malware will bypass an organization's security system and gain access to resources on that network.

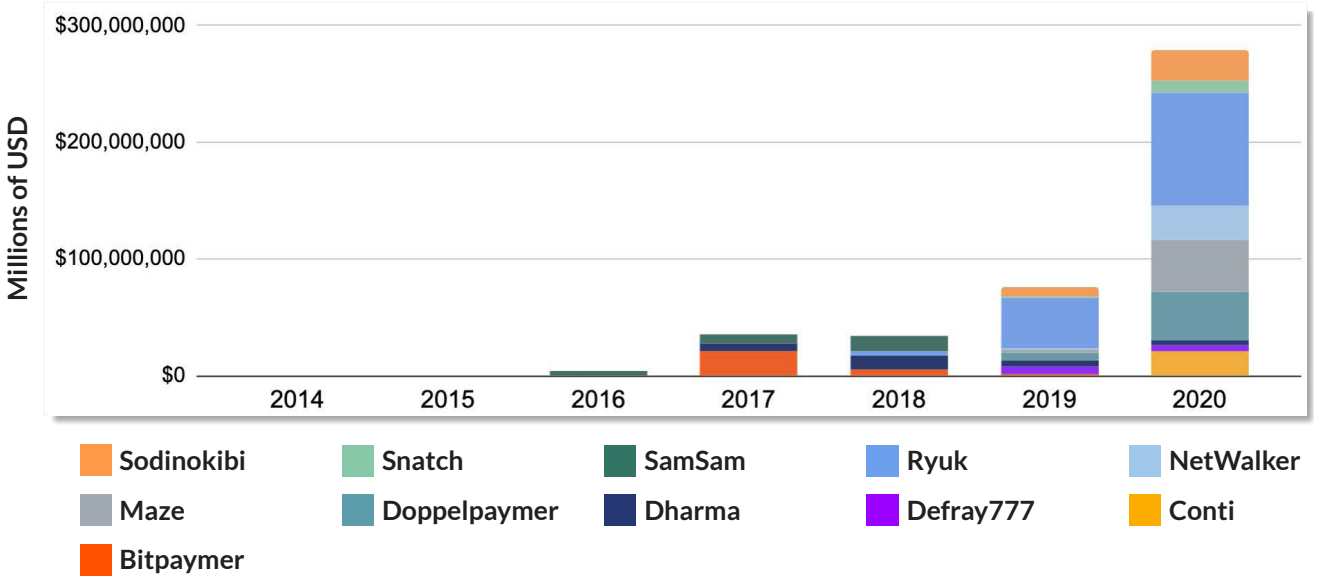
The ransomware could be obtained through a legitimate looking email with a link to a resource, or an affected file from a "work colleague", a "trusted government entity", or some other means where the victim was unaware of the true mission of the payload. Once downloaded, that user and many others can be affected (should the malware run unchecked). Ransomware can also be injected by physical or logical ports - for instance, USB devices such as unknown thumb drives or even cell phone chargers.

Another popular attack vector has been the Remote Desktop Protocol (RDP). It was the source of many ransomware attacks during 2020. Now, we must also contend with a rise in attacks of the VPN infrastructure as an entry point. Ransomware gangs used open vulnerabilities to download scripts and scan computers for targeted ransomware attacks. The key to not having these vectors exposed is to ensure the possible offending equipment is properly patched and secured.

Before these attacks became more sophisticated, payment was demanded in the form of a cashier's check, sent mainly to an offshore location. Sometimes, the perpetrator would unlock your files, sometimes not.

Today, the payment is mainly conducted via some form of cryptocurrency, which can be difficult to track. Also, the rise of Ransomware as a Service (RaaS) makes it simpler for almost anyone, typically ransomware gangs to get into the Ransomware Space.

*Top 10 ransomware strains by revenue by year, 2014-2020



Currencies included: BCH, BTC

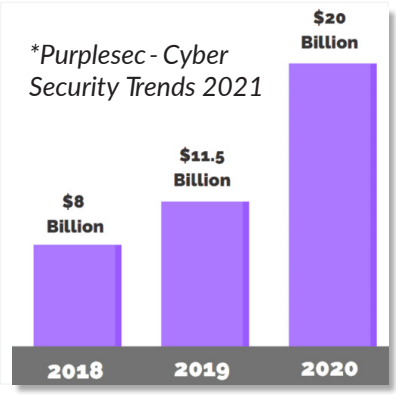
The revenue number rose 311% compared to 2019, Chainalysis said, blaming this sudden increase on "a number of new strains taking in large sums from victims" and "a few pre-existing strains drastically increasing earnings." These statistics are from their 2021 Crypto Crime Report.

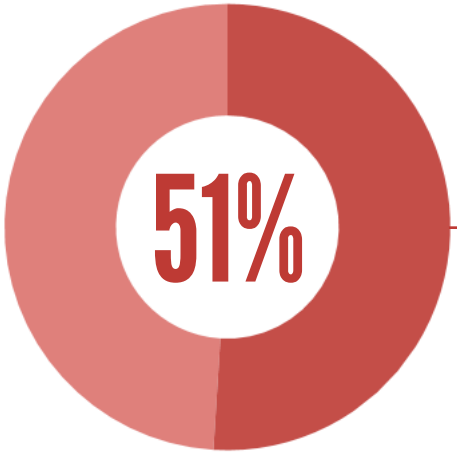
To pay or not to pay?

Do you pay, or do you learn the lesson and try and recover what data you can and move on? There is no assurance that if you pay, they'll unlock. Plus, there is the moral dilemma associated with supporting the furthering of a dark enterprise. Even if you do pay and regain access, there's no guarantee they haven't deposited some other gift that could wreak havoc in the future. Furthermore, guidance from the U.S. Dept of the Treasury, Office of Foreign Asset Control (OFAC) that make ransomware payments to threat actors are violating OFAC regulations and laws. This could lead to criminal liability.

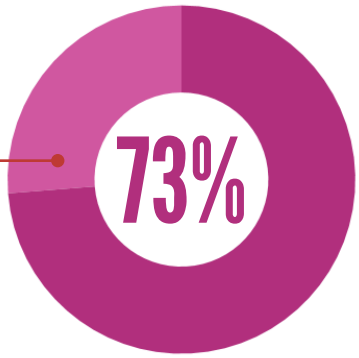
A good defense in the name of world class security software and best practice user education is the better answer. Attackers will then most likely move on to an easier prize, unless your business is the object of a targeted attack.

*Estimated global damage from ransomware.

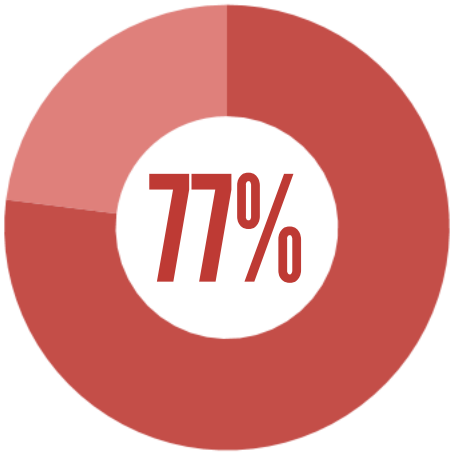




51% of global businesses are targeted by ransomware (57% in the USA)



73% of that 51% were successful



77% of successful ransomware attacks utilized fileless techniques that pass A/V

50% of businesses do not believe they can withstand a ransomware attack

*Average cost to remediate a ransomware attack.

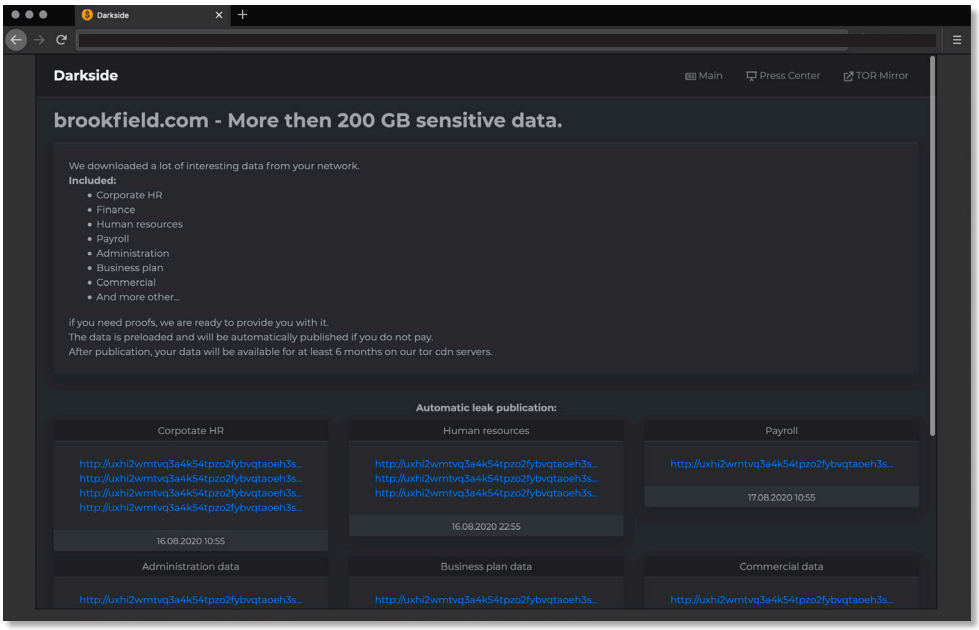
*Sophos - The State of Ransomware 2020

RECENT RANSOMWARE ATTACK PROFILES

Brookfield Residential Properties, Calgar , Canada – August 2020

Allegedly, a group noted as the "Darkside", claimed launching a ransomware attack against Brookfield. They also alleged to have copied some 200gb worth sensitive corporate data to include employee, business plans, and other unspecified information (before encrypting it) and would release it publicly unless a ransom was paid. They went on to say, "If you need proof, we are ready to provide you with it." Also, "The data is preloaded and will be automatically published if you do not pay." Specific details of the type of attack were not divulged.

**Sourced from http://darksideREDACTED[.]onion/blog/article/id/7on 2/16/2021:*



City of Lafayette, Colorado – July 2020

A ransomware cyberattack on the city's computer systems disabled several key services to include: phone service, email, online payment and reservation systems. The city recovered financial data from viable unaffected backups, and there is no evidence personal data was compromised. The city decided to pay a ransom to obtain a lockout key to avoid an extended outage, or possible loss of data. Further details about the type of cyberattack or additional remediation activities were not released.

**Image: City of Lafayette, Co.*

COMBATING RANSOMWARE WITH ZTA

Overview

Combating ransomware utilizing a Zero Trust Architecture can be accomplished by leveraging some existing technology, with additional investment depending on design requirements. By implementing the ZTA, you start by eliminating the element of trust that is found in today's typical environments. This reduces the attack surface by limiting which users and devices can access sensitive corporate resources.

For instance, implementing or taking advantage of your existing multifactor authentication environment is one element to increase the security of your network. Confirming the user's identity is one way of limiting potential damage. Know who is on your network. Another item to consider is practicing least privilege access, meaning only give the lowest level of access required devices, or users to access data. This is important because during a breach, lateral movement within the network is limited and the attack surface is therefore inherently minimized. Malware cannot be distributed across the network as a result. Microsegmentation is also an important technique creating smaller zones within the larger network to contain attacks. If a breach does happen, containment is possible. You must also consider real time monitoring to be able to detect, react, and shut down potential security incidents before they become wide spread. Swift detection, investigation, and remediation of intrusions is key to maintaining a Zero Trust Architecture.

Of course, there will be challenges to implementing ZTA. Your business may have legacy applications, a hybrid network (cloud and on prem), lack of administrative controls, etc. A good start would be to conduct a ZTA Readiness Assessment to ensure your business is prepared to implement this strategy. If not, our Architecture and Infrastructure Services Team can assist with the design and implementation. Also here at Avertium, we can assist with monitoring and responding to real time events.

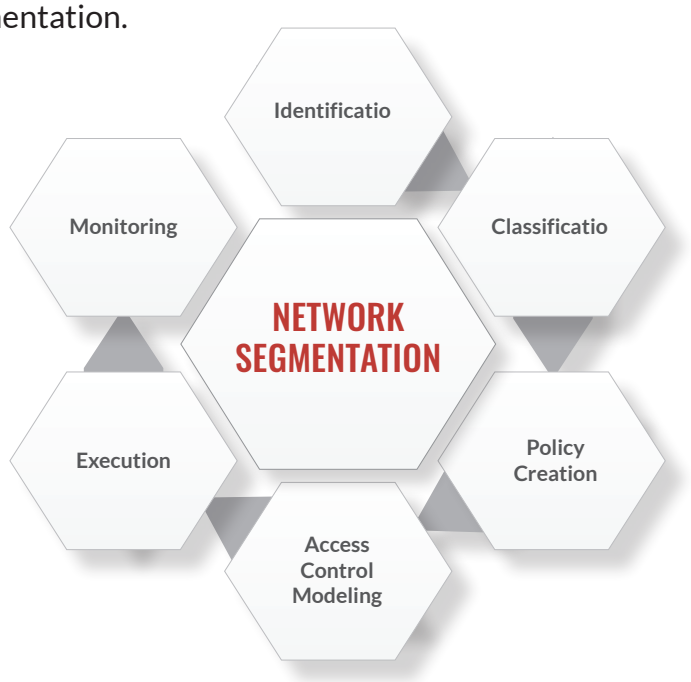
AVERTIUM CUSTOMER STORY

When a potential customer came to Avertium with a possible ransomware situation, we jumped into Digital Forensics and Incident Response (DFIR) mode:

- **We understood the cause + stopped the attack:** As it turns out, the threat actor had leveraged a VPN vulnerability exposing the credentials of domain administrators, requiring a comprehensive recovery of the organization. We quickly identified the ransomware as Netwalker, and implemented a remediation plan designed to remove the malware.

- **After the environment was secure, we turned our eyes toward prevention:** Once the environment was safe, we engaged with the customer, designing a Zero Trust Architecture to prevent a similar event from happening again.
- **We collaborated with the internal teams and legacy systems in order to architect a sustainable solution:** Working alongside the customer, we identified their network's legitimate users and devices utilizing their existing IAM Tools. With this information, we were able to establish access controls for resource access and create network or Microsegmentation.

Network segmentation is a security measure that partitions a network into sections or segments to restrict the movement of a threat and make it difficult for an attacker to gain access to valuable resources. Network segmentation is a core element of comprehensive adoption of ZTA dividing a network into multiple segments or subnets, each acting as its own small network. Avertium's approach to network segmentation projects starts with crafting a framework and strategy to ensure that the end objective of a more secure network is met.



- **We provided ongoing support through our XDR managed services offering:** This gave us the ability to continuously monitor, validate, and protect the Zero Trust Environment, watching for user and device behavior. When a reason to no longer trust someone / something presents itself through monitoring, ZTA can stop the threat and XDR can help a customer dynamically adjust to the changing circumstance. More importantly, behavioral monitoring capabilities can detect evidence that reconnaissance, or the beginnings of an attack, is underway so it can be eliminated before it becomes a major issue.

AVERTIUM'S APPROACH TO XDR

The rigorous Avertium approach to providing extended detection and response (XDR) gives our customers more visibility into data across networks, clouds, endpoints, and applications.

Using best-in-class technologies, experts at the Avertium CyberOps Centers of Excellence collect and correlate data across a wide array of data sources so that threats can be analyzed, prioritized, contained, and remediated faster and more accurately.

CONCLUSION

Zero trust and existing frameworks can be employed to reduce the attack vectors and improve your overall security posture against ransomware. With Ransomware on the rise in 2021, and forecasted to increase again in the coming years, organizations need to invest in an infrastructure to prevent the breach from initially happening. This said, a Zero Trust Architecture can improve your defense against probable ransomware attacks within your organization.

If the expertise within your company does not exist, or you simply do not have the cycles to implement the Zero Trust Architecture, Avertium, a Trusted Advisor, can assist with Architecture and Implementation Services to plan and stand up the environment. In addition, Managed Zero Trust Networking can eliminate any complexities to afford protection against ransomware and other malware attacks.

AVERTIUM APPROACH

Engineering a rigorous ZTN architecture involves significant effort and commitment, a factor that may affect your plan for adoption. Avertium works alongside you to tackle the challenges of applying an effective solution, enabling swifter implementation:

- Identifying and organizing sensitive systems and data for proper segmentation
- Ensuring legacy and/or existing system and process compatibility over peer-to-peer, hybrid cloud, and decentralized operations that break the least privilege model
- Understanding which data needs to be accessed, how it should be accessed, and by whom

Avertium is the managed security and consulting provider that people turn to when they want more than check-the-box cybersecurity. In today's threat environment, your not-so-standard processes, workflows, and vulnerabilities require more than just a standard approach to cybersecurity. You need a smarter, stronger, show-no-weakness approach. That is why more than 1,200 organizations in every sector from manufacturing and retail to healthcare and government all rely on Avertium. We bring more **rigor**, more **relevance**, and more **responsiveness** to their security posture.

More Rigor

You want a partner with deep capabilities in every cybersecurity specialty from monitoring and detection to training and compliance, and you need them to work more closely with you.

More Relevance

That gets you beyond off-the-shelf solutions and standard compliance measures to true best practices that match your specific threat e vironment and security requirements.

More Responsiveness

From highly experienced professionals who can act faster because they know you, know your systems, know your business, and know what they are doing.

AVERTIUM®

CONNECT WITH US

CyberOps Centers of Excellence
Arizona • Colorado • Tennessee

Contact Us | www.Avertium.com

#SHOWNOWEAKNESS™