

Network Obfuscation: The Secret Weapon for Protecting Your Critical Assets



Introduction

The COVID 19 pandemic accelerated digital transformation as organizations and their personnel shifted to working from home. With the migration to remote work and remote learning, cyber attacks have increased exponentially across the board, from phishing schemes to malware attacks to DDoS attacks to ransomware – the fastest growing and most damaging type of cybercrime. Attacks on state and local agencies, utilities companies, and healthcare organizations have made it clear that no organization is safe from cybercrime.

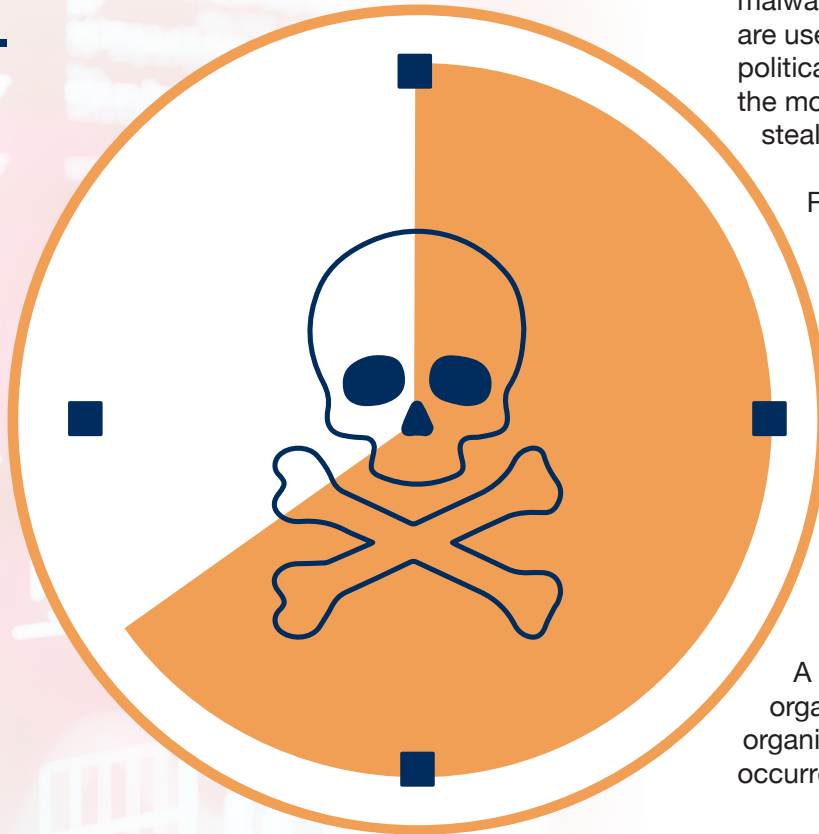
Why are we seeing an explosion in cyber attacks? How can organizations prepare and respond to this increasing threat?

In this e-book, we will look at the changing cybersecurity environment and how current security solutions can be augmented to help organizations protect their critical assets and stay one step ahead of the attackers.



Cyber attacks are increasing and evolving

**Every 39 seconds,
a cyber attack
happens.**



Every 39 seconds, a cyber attack happens.¹ Attacks are on the rise and have become the new norm across public and private sectors. Brute-force attacks are used to gain access to organizational resources in order to spread malware and steal sensitive information. Distributed denial of service attacks are used to incapacitate an organization's network as a prank or for personal, political, or business reasons. Email phishing scams continue to be one of the most successful tactics utilized by hackers to distribute malware and steal user information.

Ransomware attacks are the most damaging. They are no longer limited to requesting a ransom payment. It is a lucrative business usually operated by organized crime syndicates seeking to exfiltrate company information, the more sensitive the better. It is estimated that every 11 seconds a business suffers a ransomware attack and damages are estimated to reach \$20 billion in 2021.²

By the time the extortion demand is made, the malicious actors have been buried within an organization's networks undetected for weeks or months performing reconnaissance on the company's financial standings and crown jewels and exfiltrating large amounts of data and credentials. The damage has already been done even before the ransom is paid.

A slew of high profile, disruptive attacks on critical infrastructure organizations --- Colonial Pipeline, JBS USA and Kaseya – have left organizations and the government scrambling to answer how this could have occurred and what should be done to handle the growing threat.

1. Study by Prof. Michel Cukier, Clark School's Center for Risk and Reliability and Institute for Systems Research, University of Maryland

2. Cybersecurity Ventures, Global Ransomware Damage Costs Predicted To Reach \$20 Billion (USD) By 2021

Current security solution pitfalls



Enterprises have a plethora of tools in their security portfolio to prevent and protect their organizations from the onslaught of hackers attempting to breach their networks. The current enterprise security toolkit is focused on protecting the perimeter and endpoints with solutions like anonymous VPNs, firewalls, intrusion detection systems, and WAFs. These solutions are designed to ensure that only authorized personnel are allowed onto the network. Multi-factor authentication, least privileged access, and network segmentation provide an extra layer of security and protection to stave off insider attacks by limiting user access, reducing the overall attack surface area by dividing the network into smaller units, and lessening the severity of damage when the network is breached.

Zero Trust security has reinforced the privileged access concept by taking this one step further with the belief that no user, device, or application is to be trusted until the network is able to verify and authenticate who you are and whether you are authorized to be on the network.

But endpoints aren't the goal of an attack. They're just the first stage. Attackers breach them in order to get inside a network and find stored assets they can sell or use to conduct extortion or fraud.

If that's the case, how do organizations protect their critical assets whose compromise could cripple their operations?

Cordon off your critical assets or crown jewels

All networks have vulnerabilities, no matter how obscure; attackers can get in if they really want to. The pervasiveness of ransomware attacks is due to the increasing number of attack surfaces. For the modern organization, the attack surface is complex and massive. The larger number of endpoints, web applications, and network nodes are all possible access points through which ransomware can enter. There are simply too many attack surfaces for IT teams to defend. Despite all their best efforts, only a subset of security risks are visible to IT teams.

To protect the critical assets, they need to be separated and hidden within the enterprise networks and from the public internet. Organizations need to cordon off their most critical assets or “crown jewels” from the rest of the network and be totally hidden from the web. If cyber criminals cannot see the network resources, it is effectively protected from attack.



Network obfuscation: Your secret security weapon



Organizations can now augment their security portfolio to include a virtual obfuscation network, which protects critical assets, operations, and people from discovery in the digital domain. Network obfuscation hides servers, applications, and unified mobile communications from the public internet and seals them off from the enterprise network. Even if attackers were able to gain access to parts of enterprise network, they wouldn't be able to find people or resources within the virtual obfuscation network.

Network obfuscation uses a combination of technologies that include multi-layered encryption, dynamic IP routing, varying network pathways, and eliminating source IP addresses to hide the presence of a person, asset or resource on the public internet. With a virtual obfuscation network, the organization's critical assets can reside on a hidden server that is only accessible through the virtual obfuscation network, which itself is hidden from unauthorized users. The critical enterprise asset can be sensitive organizational information or personal information about employees and customers.

In the next section, we will discuss the different use cases that could benefit from a network obfuscation solution.

Healthcare



The
number of
healthcare
breaches
increased
55% from
2019 to 2020.

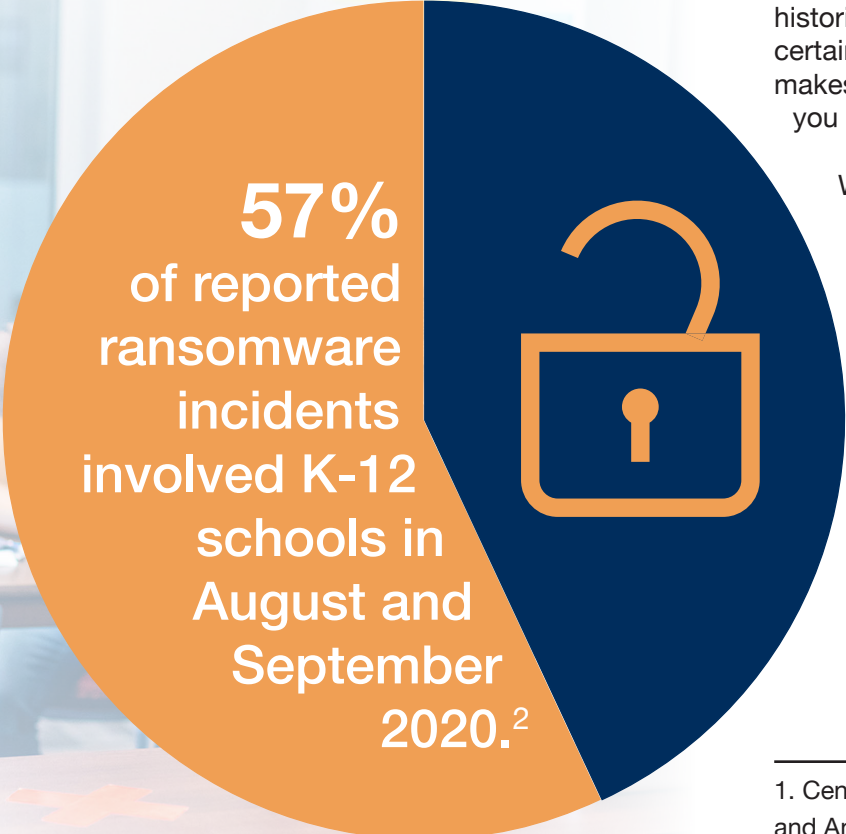
The number of healthcare breaches increased 55% from 2019 to 2020.¹ Healthcare organizations have legacy billing and procurement systems that are integrated with third-party solutions creating holes that hackers look for as easy points of ingress. In addition to the back-end systems, 56 percent of workstations on the hospital floor are using outdated operating systems, mainly Windows 7. Replacing them would be costly, but leaving them as they are could be worse.

The FBI warns that hackers are developing targeted malware and malware-less techniques to specifically exploit these old systems—so just one computer running an obsolete OS makes the entire network vulnerable to a sophisticated targeted attack.

A cloud-based obfuscation network would hide servers, applications, and unified mobile communications from the network, so even if attackers were able to enter parts of the environment through a patient wristband, stolen laptop, or firewall misconfiguration, they wouldn't be able to find the healthcare organization's crown jewels.

1. Bitglass, *Healthcare Breach Report 2021: Hacking and IT Incidents on the Rise*

K-12 organizations



57%
of reported
ransomware
incidents
involved K-12
schools in
August and
September
2020.²

Cyber attacks against K-12 organizations are expected to increase by 86%.¹ Students are high value targets for cybercriminals for their identities, which have no credit histories. When school administrators choose to block certain sites because they have a bad reputation, it only makes them more attractive to young people. How do you protect student identities while they are online?

With a virtual obfuscation network, organizations can fully encrypt data in transit from endpoint to the network, anonymize students and remove their digital footprints making them untrackable and untraceable. They can't be geolocated or targeted by advertisers.

1. Center for Internet Security's Multi-State Information Sharing and Analysis Center

2. CISA/FBI/CIS, *Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data*

Higher Education

Every year, as much as \$600 billion in IP is stolen from the United States,¹ and universities are a prime target for these crimes. Ideas flow freely in the collaborative culture of academia, and so do people – research assistants and post-docs rotate in and out, staff turns over, and new business or academic partners are brought into the mix. Few of them are aware that their work, even in the earliest stages of research, is highly valuable to those outside the project.

Using a cloud-based obfuscation network, universities can fully encrypt data, making students and faculty anonymous and eliminating their digital tracks, even when they go to legitimate websites. Large data sets used in university research are not a problem. They can be processed and stored inside the obfuscation network, unseen by anyone but the researcher working on them.



1. 2017 Report Update, *Commission on the Theft of American Intellectual Property*

Financial Services Organizations



238
percent spike in
cyber-attacks
against financial
services
organizations.

Cyber attacks are the greatest risk to financial institutions. The first half of 2020 saw a 238 percent spike in cyber attacks against these organizations¹ — and along with that came a 141 percent increase in regulatory fines. Organizations whose entire existence depends on ultra-secure data repositories and transactions, a virtual obfuscation network is an efficient and effective way to keep their data out of the hands of criminals.

Think of the obfuscation network as an impregnable vault that contains your most critical digital assets in addition to the conventional security you use on the enterprise network. Network obfuscation hides servers, applications, and unified mobile communications from the network, so even if attackers were able to enter parts of the environment through a compromised web app, stolen laptop, or firewall misconfiguration, they wouldn't be able to find your crown jewels.

1. WMWare Carbon Black, *Modern Bank Heists 3.0*, May 2020

Fraud investigators

For fraud analysts and online investigators, the public internet is a trove of valuable data that can be crucial to a case. Researching publicly available information online puts analysts in contact with toxic sources and potential threat actors. Their work can unintentionally reveal their presence on the internet, their geographic location and even their identities or — worse — exposing attack surfaces for hackers to exploit. Insurance investigators have been discovered and attacked by bad actors who were able to trace their online activities back to the home office.

Utilizing a network obfuscation solution, features like managed attribution, dynamic IP routing and multi-layer encryption can help fraud analysts and online investigators to blend into their digital environment, avoid detection, and work without fear of discovery.

Insurance investigators have been discovered and attacked by bad actors who were able to trace their online activities back to the home office.



Critical Infrastructure Sector

Organizations in critical infrastructure rely on operational technologies such as SCADA, ICS, WSANs, industrial IoT, and others to manage and optimize their industrial processes. Yet these OT systems are at greater risk now that they are increasingly connected to the internet and to enterprise IT networks. Breaches across critical infrastructure sectors are a near-weekly occurrence.

With a cloud-based obfuscation network, organizations can hide OT/IT network resources, whether they are end-user devices, sensors, servers, IoT devices, or entire network enclaves. Network obfuscation techniques can eliminate cyber-attack surfaces to ensure the most critical assets are hidden from the public internet.



State and Local Governments



\$18B

**Ransomware cost state
and local governments
over \$18B in 2020.**

Ransomware attacks cost local and state governments over \$18 billion in 2020.¹ They are one of the most targeted sectors for ransomware attacks due to vast amount of data they collect and yet they have the least resources and capabilities to protect state information assets from ransomware. Municipalities oversee water utilities, airports, and health care facilities – and a breach could interrupt services and cause massive disruptions to our daily lives.

To protect against ransomware attacks, organizations need to evaluate their systems and remove unnecessary and unsupported systems from the internet. Identify your critical systems or the crown jewels and then hide them with a virtual obfuscation network.

1. Comparitech, *Ransomware attacks on US government organizations cost \$18.9bn in 2020*

Conclusion

With the massive move to the cloud and remote work now a firmly established model, organizations are more connected than ever before and have more attack surfaces than ever before to defend. To protect this new enterprise network, organizations need to think beyond the traditional endpoint security and not limit themselves to conventional enterprise security strategies. Their strategy needs to include a network obfuscation solution that hides digital resources and users' identities and locations from detection while they are on the internet.

Operating under the philosophy that you can't exploit what you can't see, Telos Ghost[®], a cloud-based obfuscation network, hides critical network resources and the identity and location of users to ensure privacy and security as they work on the public internet.

To learn more about Telos Ghost, visit www.telos.com/telos-ghost.

