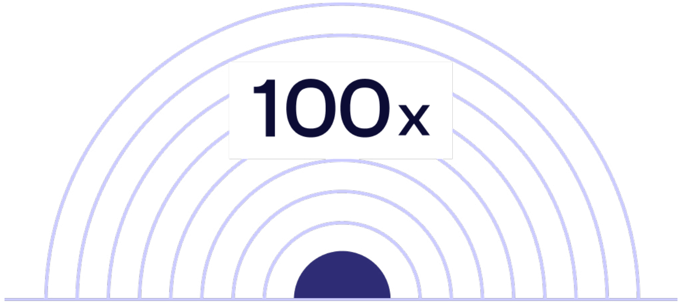
THE RANSOMWARE ELIMINATION DIET

Better Defenses Through Operational Threat Intelligence

CENTRIPETAL

EXECUTIVE SUMMARY

Cyberthreats have grown increasingly sophisticated over the last several years as professional gangs have been busy upgrading their tools and methods. Ransomware, it appears, has become their go-to attack and for good reason. As we'll see, ransomware has become big business and now ranks as the #3 type of attack. But the news isn't all bad. Organizations have learned to fight back by taking a layered approach to security and discovering how to turn threat intelligence into ThreatOps.



With neither the staff nor the resources to make good use of the event storm of alerts and notifications from the complex array of monitoring tools, ThreatOps can prevent ransomware and make your existing layered defenses 100x more effective. Keep reading to learn how your security and network teams can regain control and protect your business from increasingly sophisticated ransomware attacks.

ThreatOps is the key to making your existing layered defenses 100x more effective.

RANSOMWARE GETS INCREASINGLY POPULAR

Ransomware attacks continue to rise in popularity and now occupy the number three spot in total breaches worldwide. What's more, the rate of ransomware attacks doubled from the prior year and represented 10% of total breaches, despite the enormous attention and increased funding that goes into our collective layered security defences.[1]

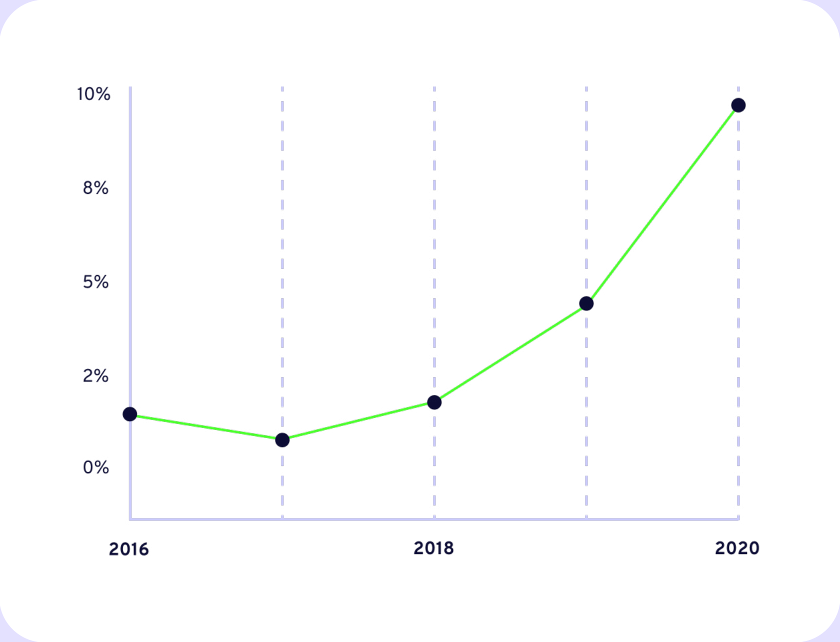
An Existential Threat to the Business

Ransomware has grown in popularity because it's effective. Cybercriminals and their victims know that a well-executed attack can cripple an organization and even put it out of business. This existential threat has reinforced for businesses the importance of backing up important data in case an attack occurs, which has been an effective defense against hackers maliciously encrypting an organization's data. However, ransomware attackers have learned to counter this simple defense by publicly shaming the organization if they fail to pay. They do this by threatening to share the sensitive information they've stolen to blackmail victims into submission.

The double-whammy of disrupting operations and public shaming is what makes ransomware attacks so attractive to cybercriminals and largely explains the surge in attacks.

The popularity of cryptocurrency has only added to the attractiveness of ransomware attacks, as attackers are finding it much easier to escape undetected by demanding payment in bitcoin. To that end, Ransomware payments through cryptocurrency totaled almost $350 million in 2020, which represented a 4x increase from 2019.

Exponential growth of ransomware breaches (Version DBIR)



[1] 2021 Verizon Data Breach Investigations Report.
[2] Chainalysis 2021 Crypto Crime Report

RECENT RANSOMWARE ATTACKS

Kaseya

IT Services USA

$70 million

Ransom Requested

Brentag

Chemicals Germany

$4.4 million

Ransom Requested

Quanta

Technology Taiwan

$50 million

Ransom Requested

Accenture

Consulting Ireland

$50 million

Ransom Requested

JBS

Food Processing USA

$11 million

Ransom Requested

Kia Motors American

Automotive USA

$20 million

Ransom Requested

Colonial Pipeline

Energy USA

$4.4 million

Ransom Requested

Acer

Technology Taiwan

$40 million

Ransom Requested

Health Service Executive (HSE)

Healthcare Ireland

$20 million

Ransom Requested

CNA Financial

Insurance USA

$40 million

Ransom Requested

TRADITIONAL THREAT INTELLIGENCE IS NOT WORKING

Cyber threat intelligence (CTI) is what cyber threat information becomes once it has been collected, evaluated in the context of its source and reliability, and analyzed through rigorous and structured tradecraft techniques by those with substantive expertise and access to all-source information.[3] CTI has held the promise of protecting organizations against malware attacks, including ransomware. Despite two generations of evolving cyber threat intelligence tools, however, companies that deploy them are still getting hacked and still spending liberally on tools, feeds, and people.

Traditional threat intelligence is only as good as your ability to use it

If you think about it, it's not surprising that traditional solutions aren't preventing costly breaches. Most firms use threat intelligence to educate themselves on the latest threats and attack motives, while others passively use indicators of compromise (IoCs) to alert them to take corrective action after an incident occurs.

Plus, with billions of IoCs today and more being added daily, the IT teams responsible for implementing these solutions simply can't keep up. In fact, businesses are making conscious decisions to ignore what their CTI solutions are guiding them to do.
Let's take a look at some of the biggest reasons for this.

Businesses can't keep up with the volume, variety, and velocity of threats, despite their layered security defenses.

[3] Center for Internet Security

TRADITIONAL THREAT INTELLIGENCE IS NOT WORKING

Issues Preventing Effective Use of Threat Intelligence:

01. The variety of global CTI vendors requires using multiple proprietary feeds to get full coverage

02. Deploying numerous feeds is essential but costly to maintain

03. Triaging the volume and variety of threats doesn’t scale

04. IT teams don’t have the cybersecurity expertise to analyze and systematically block suspicious traffic

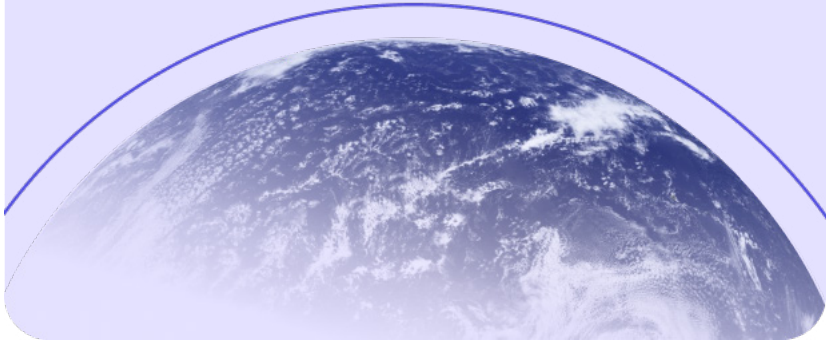
05. IT teams often ignore legitimate threats because “false positives” lead to poor network performance

06. Some vendors are slow to update IoC lists, resulting in overly static lists

07. Organizations place blind trust signature-based solutions like firewalls, IDS/IPS tools that don’t scale

OPERATIONALIZING THREAT INTELLIGENCE

Considering the issues with traditional threat intelligence, it's time to think differently. There's no reason organizations can't make full use of the collective intelligence amassed by the global CTI community. To do that, we need solutions that can scale to effectively analyze every known IoC, billions of them. Only then will we be able to realize the true potential of the global threat intelligence community.



Transitioning from Threat Intelligence to ThreatOps

Two generations of threat intelligence solutions have given us great visibility into an endless stream of cyberthreats but also have exposed the scalability challenge of analyzing billions of threat indicators pounding away at our networks. What we need is a way to operationalize threat intelligence to enable organizations to secure at scale by leveraging all relevant threat feeds to shield it from all threats and in real-time.

This means eliminating ALL known threats mapped by the global threat intelligence community, as well as quickly acting on emerging and zero-day threats. Doing so will ensure that even the most innocuous threats are eliminated just as efficiently as the most dangerous emerging ones.

ThreatOps is the process of operationalizing threat intelligence to shield against all known and emerging attacks.

OVERCOMING THE LIMITATIONS OF TRADITIONAL THREAT INTELLIGENCE

By evolving from traditional threat intelligence to ThreatOps, we find a path to overcome the limitations of traditional solutions. Organizations will be able to economically use multiple, relevant threat feeds simultaneously to take advantage of the global CTI community and systematically shield against all known threats while also defending more effectively against evolving zero-day threats.

Furthermore, a capable ThreatOps solution should include experienced threat hunters trained to analyze emerging threats in the context of an organization's business. Delivered as a service, ThreatOps would alleviate much of the anxiety of overworked, understaffed, and underfunded security teams who have been struggling with this for as long as we can remember.

Operationalizing threat intelligence in this way will not only provide better security but also end the practice of choosing between blocking suspicious traffic and meeting network performance service level agreements.

ThreatOps can finally end the practice of choosing between blocking suspicious traffic and meeting network performance SLAs.

SHIFTING DEFENSES TO THE LEFT WITH THREATOPS

It's important to recognize that ransomware is simply an increasingly popular type of malware. Looking at it this way can help organizations counter it by combining existing defense-in-depth tactics and a ThreatOps mindset.

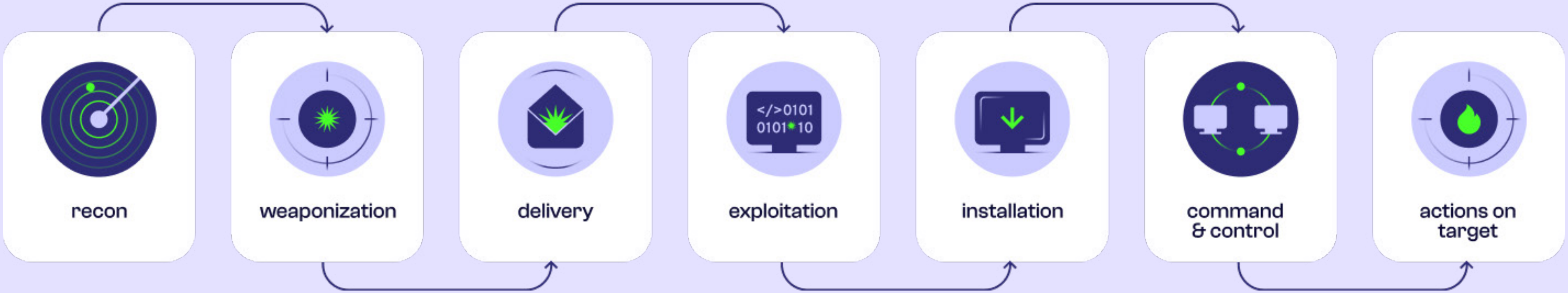
To that end, we believe ransomware attacks can be prevented largely by shifting defenses further "to the left" to recognize malicious intent long before any malware is weaponized against the target organization.

Operationalizing threat intelligence in this way would go a long way in identifying and shielding the organization against any IoCs that can rapidly evolve into a real threat if left unchecked.

Such a solution would continuously monitor inbound and outbound traffic for any sign of latent threats that might mature into something bigger. To that end, looking through the lens of the Cyber Kill Chain can help organizations understand how ThreatOps can eliminate known and zero-day threats at every stage of development.

Ransomware and the Cyber Kill Chain

The Cyber Kill Chain was developed by Lockheed Martin as a framework to help organizations understand the different steps cybercriminals must go through to conduct a successful cyberattack on a target. Mapping our ThreatOps model to this framework can help identify which steps will be most effective in preventing ransomware attacks.



THREATOPS AND THE CYBER KILL CHAIN

The Cyber Kill Chain includes seven sequential steps criminals must complete to execute a successful attack. They extend from early reconnaissance on a target to identify vulnerabilities all the way through the eventual launch of an attack. In this context, we know that the earlier an organization can recognize suspicious activity the better they can defend against it. This is what we mean by shifting defenses to the left. But even when their defenses don’t pick up on the early indicators, emerging attacks can be thwarted by applying ThreatOps across the subsequent links in the chain.

Before we dive deeper into this, however, let’s review the various links in the chain in the context of a ransomware attack:

1. Reconnassiance

In this early phase, criminals use web crawlers to identify vulnerabilities by scanning for open ports on connected systems and devices.

2. Weaponiazation

Develop exploit to deliver through the unprotected system identified in Reconnaissance.

3. Delivery

Deliver ransomware payload to target organization through the unprotected system.

4. Exploitation

Exploiting the vulnerability in the unprotected system to execute code on the system.

THREATOPS AND THE CYBER KILL CHAIN

The Cyber Kill Chain includes seven sequential steps criminals must complete to execute a successful attack. They extend from early reconnaissance on a target to identify vulnerabilities all the way through the eventual launch of an attack. In this context, we know that the earlier an organization can recognize suspicious activity the better they can defend against it. This is what we mean by shifting defenses to the left. But even when their defenses don’t pick up on the early indicators, emerging attacks can be thwarted by applying ThreatOps across the subsequent links in the chain.

Before we dive deeper into this, however, let’s review the various links in the chain in the context of a ransomware attack:

5. Installation

Ransomware is installed on the target system.

6. Command & Control

An encrypted channel is created between the infected system and an external system of the attacker.

7. Actions on Target

Enterprise data on the target system is exfiltrated and encrypted, and the victim is notified about ransom terms.

APPLYING THREATOPS AT THE RECONNAISSANCE PHASE

Each phase completed by a would-be attacker gets them closer to a collecting their ransom. More phases means more opportunities to stymie an attack if we have a solution that can recognize IoCs along the way. Let's take a look at which phases would be helpful in this way.

Eliminating threats in the Reconnaissance phase

The best approach is to eliminate potential threats as early as possible before they can evolve into something bigger. To that end, recognizing suspicious activity in the furthest-left phase, Reconnaissance, will greatly reduce the potential exposure to attacks later on.

In our ransomware example, we would use ThreatOps to inspect inbound traffic from any webcrawlers or spiderbots that are scanning the ports on our external-facing systems. If we can determine that these crawlers are related to an existing IoC we know about or if we jointly determine that they are not relevant to the business, we can systematically and automatically shield our organization from them.

Operationalizing threat intelligence in this way requires that we assign a confidence level to every IoC in our ThreatOps solution in real-time. We automatically shield network traffic above a certain confidence level and closely monitor (and log) those that don't meet that threshold yet.

Cyber Kill Chain

Reconnassiance. In this early phase, criminals use web crawlers to identify vulnerabilities by scanning for open ports on connected systems and devices.

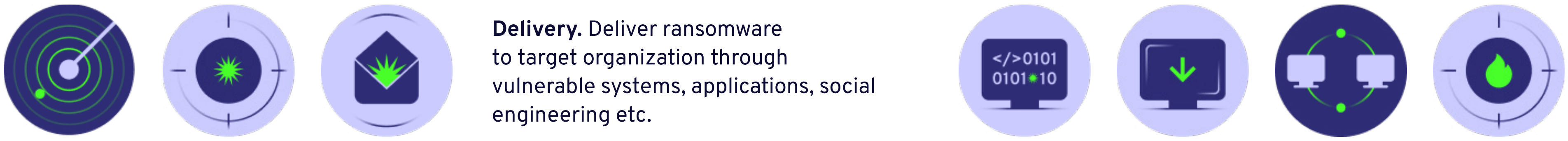
SHIELDING SUSPICIOUS TRAFFIC AT THE DELIVERY PHASE

Applying ThreatOps at the Delivery phase

Similar to recognizing and shielding potential threats at the Reconnaissance phase, we'll want to deploy ThreatOps to keep an eye out for suspicious network traffic in the Delivery phase. By inspecting inbound traffic in the context of known IoCs published in the threat feeds to which we subscribe, we can automatically shield any suspicious traffic that meets the confidence level we defined for our organization.

In our ransomware example, we would recognize when a system with a questionable domain or IP address is attempting to connect to one of our systems. If we don't flag the domain or IP address as suspicious, our ThreatOps solution should still be able to spot other anomalies or IoCs once the connection is made. This might include IoCs recognized in the data packets that could help us identify a potential threat. If this happens, we automatically terminate the connection to ensure operations resume as normal.

Cyber Kill Chain



Delivery. Deliver ransomware to target organization through vulnerable systems, applications, social engineering etc.

PREVENTING CONNECTIONS TO A COMMAND & CONTROL SERVER

Neutralizing threats in the C&C phase

In the Command & Control phase of the Cyber Kill Chain, bad actors establish an encrypted connection from a victim's infected server to an external server that they control. ThreatOps can be useful here to recognize and shield both inbound and outbound traffic flagged as a known IoC by a threat intelligence vendor.

In our example, we would recognize traffic going to and from the questionable domain or IP address of the attacker's Command & Control server and automatically sever the connection. Without a ThreatOps solution that can automatically recognize and shield outbound network traffic, in addition to inbound traffic, we would be blind to the exfiltration of sensitive data.

Cyber Kill Chain

</>0101
0101*10

Command & Control. Encrypted connection is established between infected internal systems and attackers external C&C server.

APPLYING THREAT OPS AT THE ACTION ON TARGET PHASE

Neutralizing threats in the Action on Target phase

Once an attacker establishes a solid toehold in the victim's environment with an encrypted connection to their C&C server, they are free to extract data and/or disrupt operations on their target. In our ransomware example, the attacker either encrypts the data on our server or prevents access to it to disrupt operations. The only way to recover the data or resume operations is to pay the ransom.

Operationalizing threat intelligence at this phase would allow us to identify any anomalous behavior or outbound traffic to a suspicious server associated with an IoC tracked by one of our intelligence feeds. An effective ThreatOps solution would automatically sever the connection to prevent an exfiltration of data or disruption of our operations.

Cyber Kill Chain

</>0101
0101✱10

Actions on target. Data on target system is encrypted and victim is notified about ransom terms for remediation.

IMPLEMENTING THREATOPS IN YOUR EXISTING ENVIRONMENT

It's important to think of ThreatOps as an enabler for your existing security, rather than a disruptor. Most organizations are reluctant to dismantle and redesign their layered security stacks, given the concerns over creating new vulnerabilities associated with such a makeover.

Instead, an effective ThreatOps solution that automatically shields high-confidence threats based on known IoCs makes firewalls, IDS systems, and SIEMs exponentially more effective. In other words, by greatly reducing the suspicious and superfluous traffic constantly bombarding the network, these other security tools are better positioned to perform the job they were designed to do.

Such an environment will not only provide better security for the organization but also provide better economics across the entire security stack.

THREATOPS CAN REDUCE THE GROWING CYBERSKILLS SHORTAGE

As we discussed earlier, an effective ThreatOps solution provides two levels of protection.

The first is the automatic shielding of known IoCs mapped by the global threat intelligence community. The second is the presence of a skilled team of experienced threat hunters that can help monitor and analyze emerging and zero- day threats in the context of a particular business.

The first part can be accomplished by a platform that scales to consume and process every threat feed in real-time. The second part, however, adds the human knowledge and expertise that most organizations can't provide directly. Those who can find their security analyst overwhelmed by the sheer volume of intelligence that prevents them from doing the job they were chartered to do.

Most security analysts are so overwhelmed by the time it takes to analyze log files and intelligence alerts that they can hardly maintain a current list of rules and policies to protect against even rudimentary threats. Having an experienced team of threat hunters who can supplement or completely offload the burden from their internal team will help ensure all potential threats will be carefully examined. This will, no doubt, free up time for internal teams to spend on other valuable business initiatives.

IMPLEMENTING THREATOPS WITH CENTRIPETAL CLEANINTERNET®

Centripetal has been an active part of the threat intelligence community since the early days and have seen it evolve over two generations. Over that time, we've seen the limitations of traditional solutions that theoretically should provide an adequate solution but fail in practice.

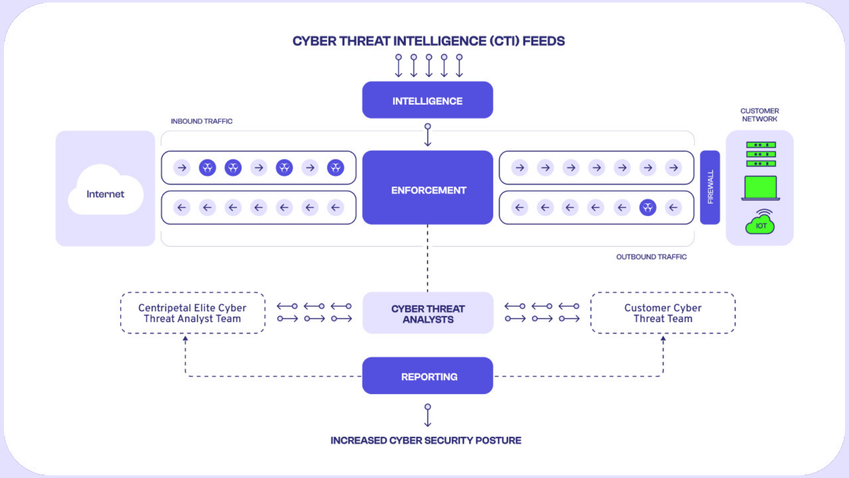
That's why we designed the Centripetal CleanINTERNET solution. Not only can it provide a higher level of security for an organization, but it alleviates the economic burden and shortage of skills that every organization faces today. And it makes existing security inspection strategies 100x more efficient and cost effective.

First, CleanINTERNET elevates your security posture by working at massive scale and machine speed to proactively shield you from 99% of globally-mapped threats identified by the threat intelligence community in near real time.

This comprehensive threat shielding enables overburdened SecOps teams to work with our dedicated team of experienced threat hunters to focus on the remaining 1% of emerging and zero-day threats.

Delivered as a managed cybersecurity service, CleanINTERNET also greatly reduces the cost and implementation traditionally associated with advanced threat protection.

CENTRIPETAL CleanINTERNET®

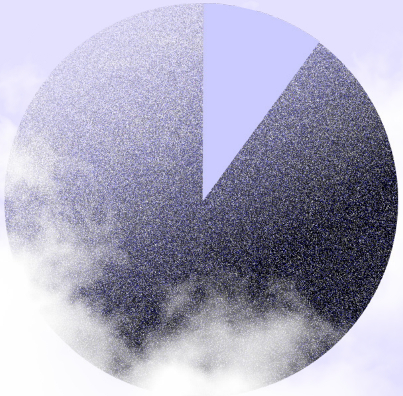

CYBER THREAT INTELLIGENCE (CTI) FEEDS
INTELLIGENCE
INBOUND TRAFFIC
CUSTOMER NETWORK
Internet
ENFORCEMENT
FIREWALL
IOT
OUTBOUND TRAFFIC
Centripetal Elite Cyber Threat Analyst Team
CYBER THREAT ANALYSTS
Customer Cyber Threat Team
REPORTING
INCREASED CYBER SECURITY POSTURE

To learn more or to schedule a demo click here →

BONUS CONTENT

What to do if you're hit by a ransomware attack?

Ransomware attacks make up 10% of total cybersecurity breaches worldwide[1].



High-profile attacks on governments, banks, and critical infrastructure often make the news, but small and mid-sized organizations are no less at risk of ransomware, with cyber criminals now shifting their campaigns to fly under the radar of law enforcement[2].

While reports frequently focus on the regularity and consequences of ransomware attacks, businesses can be left unsure of exactly what to do if they spot the signs of one.

If you find yourself in this scenario, it's important to act fast and not to panic. We've prepared a simple Ransomware Attack Checklist to help guide you in planning your response.

By following this checklist, you can notify the right bodies immediately, minimize the damage to your business, and better prepare your team for future threats.

Download checklist →

[1] https://www.verizon.com/business/resources/reports/dbir/
[2] https://www.itpro.co.uk/security/ransomware/361853/ransomware-groups-will-target-smaller-businesses-in-2022

RANSOMWARE ATTACK CHECKLIST

Work through the following steps for an effective response:

1. Validate that the alert is not a false positive.

Organizations spend an unbelievable amount of time and resources on false positives that put them on high alert for nothing.

2. Isolate all infected systems.

Identify and isolate all infected systems (mapped by known indicators of compromise) and disconnect all data backups from the network. Notify employees about any emails, links, or attachments that led to the attack.

3. Identify the key aspects of the attack.

Collect the relevant log files, identify the initial attack vector, and inventory all infected machines. Hire a 3rd-party Incident Response team if expertise doesn't exist internally.

4. Notify law enforcement.

Notify Law Enforcement of initial breach via any of the following links and organizations and follow instructions from them:

A.) CISA (Cybersecurity & Infrastructure Security Agency): Submit a report: https://www.cisa.gov/uscert/report

B.) FBI - Call your local field office: https://www.fbi.gov/contact-us/field-offices

C.) ICCC (Internet Crime Complaint Center IC3): https://ransomware.ic3.gov/default.aspx

5. Remediate and restore the affected assets.

Fix the initial attack vector to prevent re-compromise. Re-image and validate the security of all compromised systems with automated scanning software. Restore all the copies of affected files from clean backups. Scan all systems again to ensure they are clean, then reconnect them to the network.

6. Review lessons learned and make adjustments.

Conduct a post-mortem on the incident to improve the organization's defenses, processes, response, and training.

CENTRIPETAL

After working on secure communications systems for the Department of Defense, Centripetal's Founder and team used their experience in government security to develop CleanINTERNET – the first threat intelligence gateway on the market. CleanINTERNET was built to provide cost-effective, seamless, and scalable cyber threat intelligence to businesses, no matter their size or sector.

CleanINTERNET works at massive scale and machine speed to dynamically shield businesses from every known cyber threat identified by the global threat intelligence community. Our solution goes far beyond detection, offering automated threat shielding and an elite team of threat hunting specialists to provide businesses with real-time protection with Advanced Threat Detection

centripetal.ai