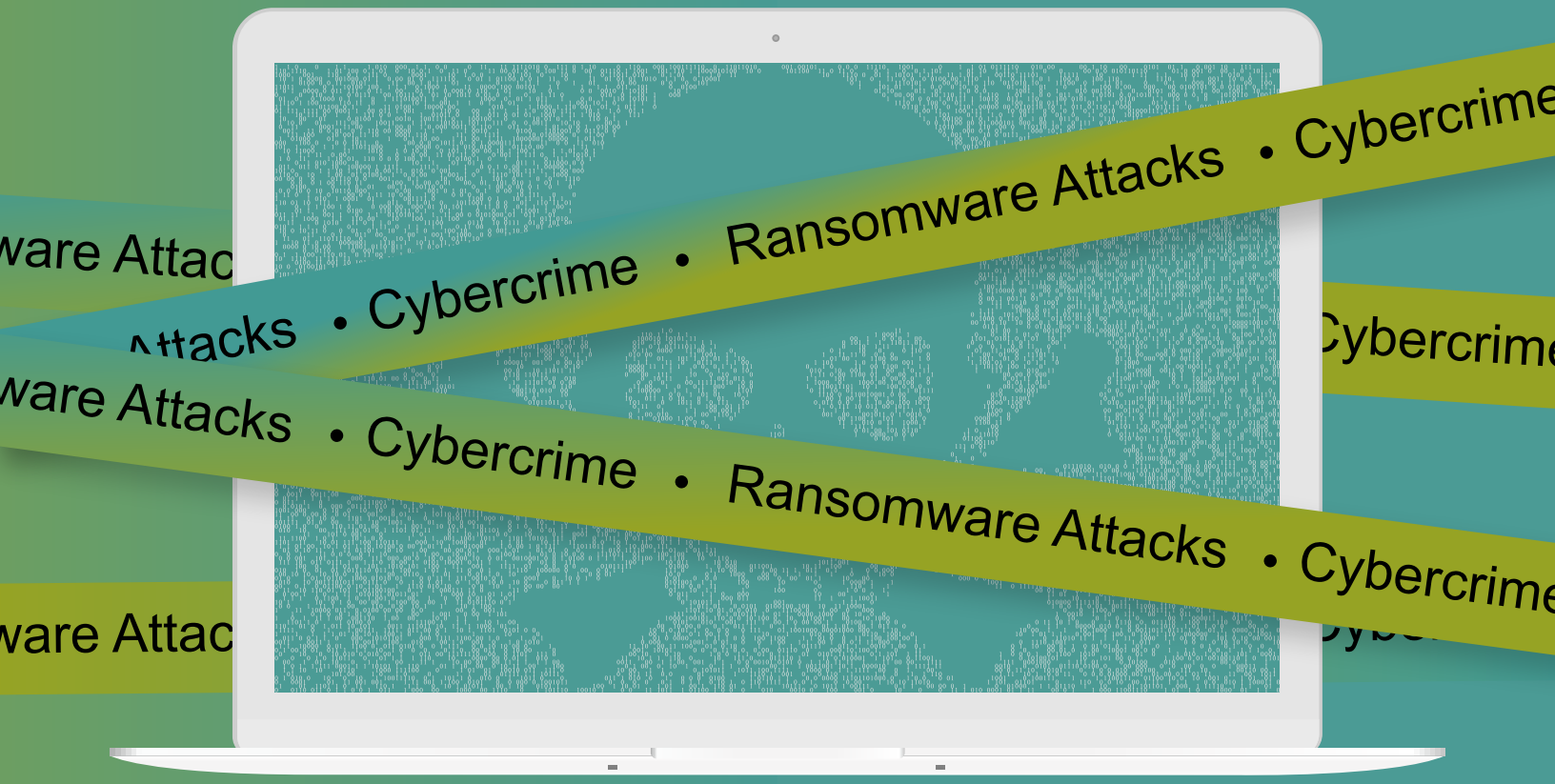
ōrdr

THE RISE OF CYBERCRIME

How CyberInsurance May Have Inadvertently Spurred The Growth in Ransomware Attacks



ABSTRACT

Cybercrime is on the rise, hitting more and more organizations and causing ever-greater damage to its victims. The causes are many, including greater technological sophistication on the part of the threat actors and a growing underground supply of cybercrime tools and alliances. Paradoxically, insurance companies may have made the situation worse by offering coverage for cyber crimes and possibly even covering costs associated with ransom payments, remediation, and recovery. In this ebook, Ordr along with former Gartner analyst and Ordr advisor Brad LaPorte investigate how we have come to the current situation, and provide best practices to secure against ransomware.

UNINTENDED CONSEQUENCES: RANSOMWARE, INSURANCE, AND INCENTIVES FOR LAX CYBERSECURITY MEASURES

Economists have a polite euphemism for the phenomenon of plans that backfire on the planners: These failures are said to have "unintended consequences." The planners took measures to solve a problem, but instead made the problem worse, created an additional problem, or both.

"Unintended consequences" now appears to describe the insurance industry's efforts to prevent organizations from suffering undue financial damages from cyber attacks. The cyberattack policies they've offered have created incentives for even more attacks and, ultimately, greater aggregate harm.

Not only are cybercriminals being richly compensated for their assaults, they're able to use more weaponry and find easier targets than in the past. Is there a ready solution? A silver bullet that will keep your organization safe?

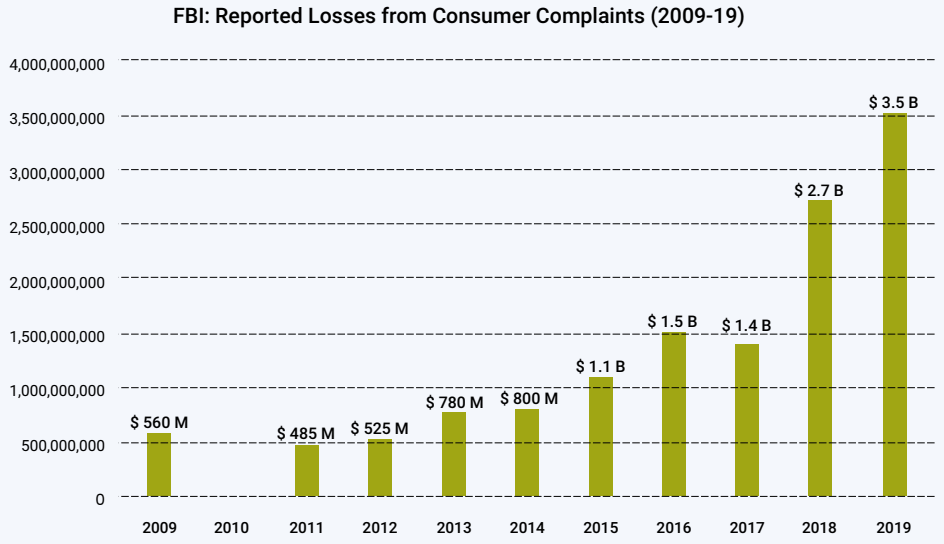
Sadly, no. The issue is complex and multifaceted. But we cannot ignore it.

This document takes a close look at how we have come to this state of affairs and equip readers with the knowledge we believe is needed to avoid falling into a false sense of security about cybercrime. With awareness of the dangers, you're at least in a better position to think through what actions you need to take – so you don't suffer "unintended consequences" of your own.

CYBERCRIME TRENDS UNTIL NOVEMBER 2019

Cyber attacks are nothing new and can be dated back to the early days of computers, picking up steam as personal computers became ubiquitous in the 1980s and accelerating dramatically with the increasing interconnectivity in the decades since. The past several years have seen the trend rise steadily, as hacking became far more than a pastime for bored youths trying to stir up trouble. Serious criminal enterprises saw an opportunity to grab the cash with relatively little resource investment. State actors saw cyberattacks as a new form of warfare and a strategic method of undermining their geopolitical rivals.

HERE'S ONE CHART SHOWING THE TREND IN CONSUMER COMPLAINTS DUE TO CYBERCRIME:



Source: InfoSec Insights

A FEW HIGHLIGHTS OF THE TYPES OF ATTACKS THAT GREW DURING THAT PERIOD:

$26 billion lost to BEC/EAC scams: The FBI's IC3 estimated that more than $26 billion was lost between June 2016 and July 2019 due to business email compromise/email account compromise (BEC/EAC) scams.

$678 million stolen by North Korea: In March 2019, the UN Security Council reported more than $678 million in foreign currency and cryptocurrency theft by North Korea between 2015 and 2018. Nation-state actors attempted to steal $1 billion via state-sponsored hacking of companies and cryptocurrency exchanges from organizations around the world.

400% increase in threats to Mac devices: In its 2020 State of Malware Report, Malwarebytes wrote that the number of threats against Apple Mac devices increased by 400% from 2018 to 2019. They reported an average of 11 threats per Mac device, which was nearly double the 5.8 threat average on Windows endpoint devices. As Malwarebytes framed the situation, "Mac users … can no longer say that their beloved systems are immune from malware."

Nearly 1 billion web-based cyberattacks repelled: Kaspersky asserted that 975,491,360 browser-based attacks from around the world were halted by its products between November 2018 and October 2019. The same data also indicated that 273,782,113 unique URLs were discovered to be malicious.

In an excellent compilation of the trends from 2013 to 2019, Brandon Levene, of the cybersecurity firm Chronicle Security, highlighted the use of "crimeware" as part of the power behind the trends. A type of malware designed to automate – and thus greatly increase the range – of cybercrime, Levene warned of its power and perniciousness. In his prescient September 2019 report, Levene alleged:

- The crimeware risk was underestimated and, without countermeasures, attacks would grow in impact, scale and costs;
- The prevalence and frequency of crimeware had desensitized security teams, leading to a dangerous fatigue in efforts to combat it;
- Law enforcement efficacy diminishes over time;
- Attacks were shifting from consumer to corporate targets as the attackers gained sophistication in their tools and techniques; and, most significantly,
- The low cost and high rewards of volume attacks encouraged more sophisticated and targeted crimeware.

Before we look at how that last point came to be particularly problematic, let's look at how the attackers were given even more incentives to unleash their assaults.

TWO KEY ELEMENTS: INSURANCE COVERAGE AND AN UNTRACEABLE CURRENCY

As ransomware became an easy way for cybercriminals to extract money from various organizations, insurance companies saw an opportunity to offer a new class of policies to vulnerable institutions. If a company had to pay the attackers to regain control of their databases or other portions of their IT systems, the insurance company would foot the bill.

As we noted earlier, this essentially gave cyber criminals even more reason to attack, knowing that their victims would be able to pay by drawing upon their insurance policies. The world of economics is full of examples of such misplaced incentives. For example, governments of earlier centuries tried to control pest infestations by paying citizens to kill the creatures, collecting upon presentation of the dead bodies. Rewarded as such, people started breeding the pests – adding to their income but also to the pest population.

More pertinent, perhaps, for the sake of this discussion is a subset of the law of unintended consequences – "risk compensation." That is, when changes are made that are designed to reduce harm, people may engage in riskier behavior than before. Take the implementation of car safety features and requirements. Studies show that drivers often drive more aggressively and dangerously in vehicles equipped with anti-lock brakes and seat belts, confident that the devices will protect them in the case of an accident.

In the case of cybercrime insurance policies, it stands to reason that overworked security teams, worn down by an onslaught of crimeware, would be less cautious if they knew their organizations were covered against losses. To be sure, this is a supposition that would be difficult to prove, because no security team wants to admit to such an attitude. But the response is understandable.

Throwing money at the problem doesn't work well in the absence of a well-reasoned policy, of course. But there was another factor at play that is relatively new to economic analyses: the emergence of digital currencies, specifically bitcoin.

Because bitcoin is not government regulated, but rather a private method of exchange, institutions lack a ready mechanism to trace a transaction. If the actors demanding a ransom after taking control of a database were paid with conventional financial instruments, law enforcement agents would be able to quickly identify them by – as the expression goes – following the money. With a bitcoin payment, once the ransom has been paid, the extortionists can disappear without leaving any tell-tale financial trails.

NOVEMBER 2019: THE TIPPING POINT IN THE ANNALS OF CYBERCRIME

The first ransomware attacks received relatively little attention because the victims of the attacks didn't want to embarrass themselves by admitting their defenses had been successfully breached. As word got around, a new defense strategy emerged: Back up your data and information continually to eliminate the leverage used by cyberextortionists. Cloud backups in particular, made this technically feasible. If hackers demanded payment for restoration, you simply told them that you didn't need the files because you had duplicates. In November 2019, a criminal group called Maze pioneered a new technique called double extortion that didn't give victim organizations an easy way out. Maze's technique was to grab sensitive information and demand financial compensation. Even if a company had backups, the ransomware perpetrators would release the sensitive data to the public if payment wasn't received.

This created a problem that companies found difficult to negotiate with while also finding themselves in a compromising position. There are 35 ransomware groups identified as having used the double extortion tactic, with a guarantee that more will follow suit.

"The incorporation of double extortion is a turning point in the ongoing evolution of ransomware. Modern ransomware attacks follow the same modus operandi: Encrypt the targeted organizations' files and demand payment in exchange for access restoration. However, since there is no guarantee that cybercriminals will keep their word, some organizations opt not to pay ransom, especially if they keep backup files anyway.

"But in late 2019, Maze pioneered the double extortion technique with a demand that was harder to ignore: Pay up, or the ransomware operators would publicly release the victims' data.

"To date, we have spotted 35 ransomware families that have employed double extortion — and the list just keeps growing. It's not difficult to see why: While loss of access to files alone already puts heavy pressure on affected organizations to yield to ransom demands, the added threat of public exposure further tightens the noose, especially if classified information is on the line."

Source: Trend Micro

This new methodology was the catalyst for an even greater onslaught. But wait! There's more!

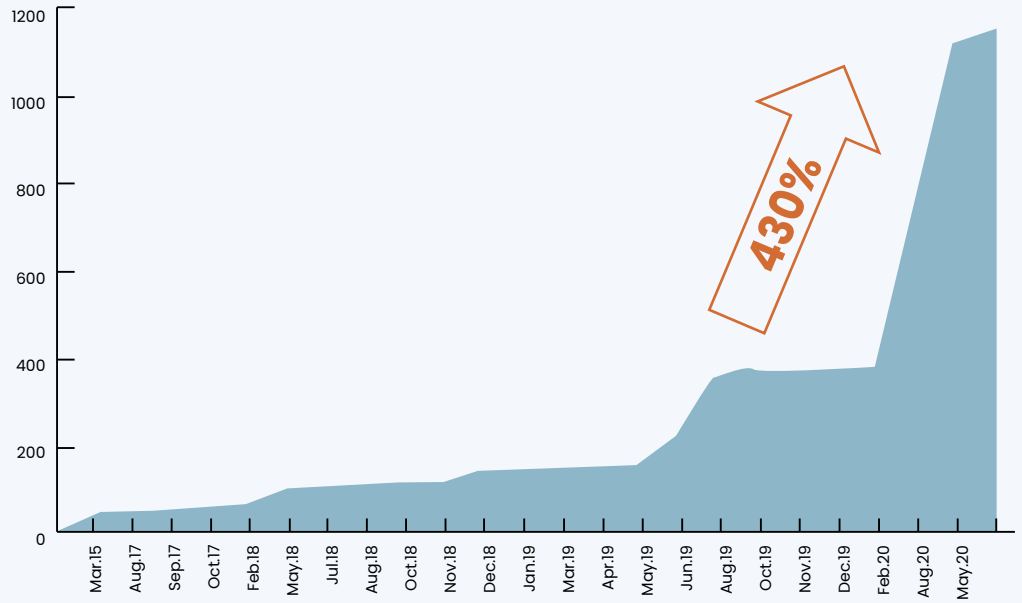
THE SOFTWARE SUPPLY CHAIN ENTRY POINT

As their tools became more powerful, so did cybercriminals' strategic planning. They saw a new opportunity in how organizations began relying on software vendors to provide IT capabilities they couldn't effectively develop on their own.

By infiltrating a software vendor's network and employing malicious code to compromise the software, malware is sent to the vendor's customers, compromising those customers' data or systems. The infiltration can come when a company first acquires the vendor's software or in subsequent actions, such as through a software patch or hotfix. In these cases, the compromise still occurs prior to the patch or hotfix entering the customer's network. This is referred to as going "upstream" in the supply chain to compromise systems earlier in the software distribution process.

NEXT GENERATION SOFTWARE SUPPLY CHAIN ATTACKS (2015-2020)

Typosquatting, Malicious Code Injection, and Tool Tampering



These types of attacks affect all users of the compromised software, and can have widespread consequences for all software customers. It's an easy multiplier for cybercriminals – attacking one target and potentially reaching thousands.

THE ZERO-DAY MALWARE THREAT

And finally, cybercriminals have learned how to increasingly deploy new malware not previously identified that can do their dirty work without being detected for days, weeks, months, or even years. These are known as zero-day exploits (zero-days) – hacking methods that have given zero warning of their presence, as opposed to those that have been previously identified and defended against already.

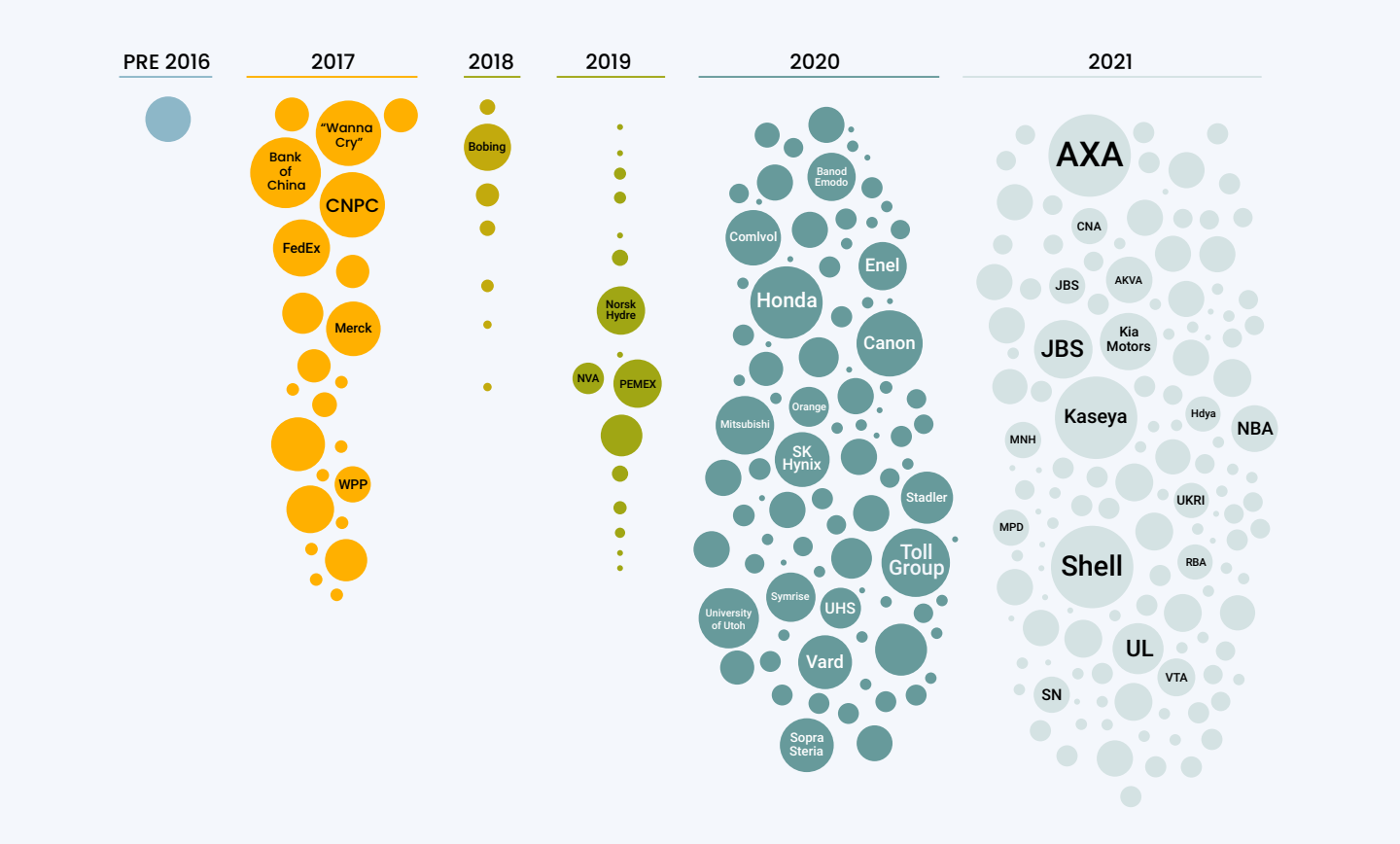
The cybercrime market for zero-days appears to have grown tremendously in value in the past few years – just as a stealth bomber would necessarily be prized over one that could be readily detected by radar systems.

DATA BREACHES SINCE NOVEMBER 2019

To be clear, attacks had hardly plateaued in the years before the November 2019 escalation. In its "Cost of Cybercrime" study, Accenture ran the numbers and found that security breaches had grown by 67 percent from 2013 to 2018.

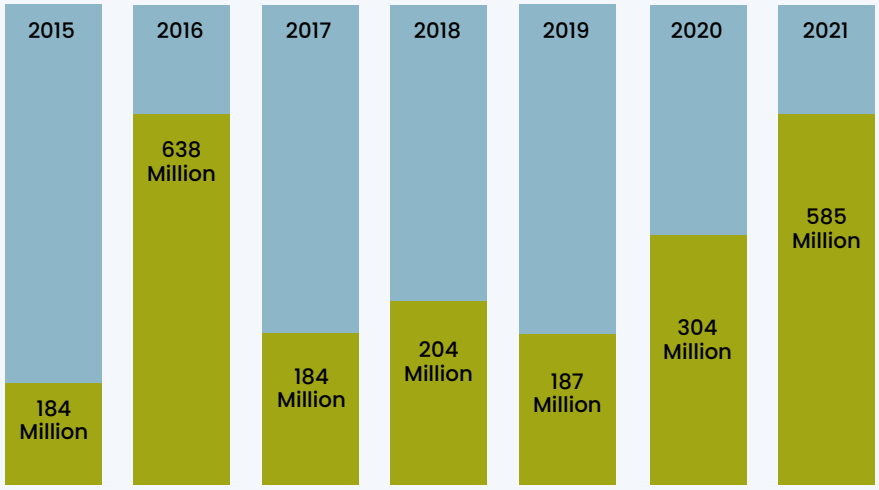
But attacks skyrocketed shortly after the November 2019 double-exposure development. Security Boulevard reported that, in the first six months of 2020, more cyberattacks occurred than in all of 2019. All signs indicated it would only get worse throughout 2021 – and it did.

RANSOMWARE ATTACKS

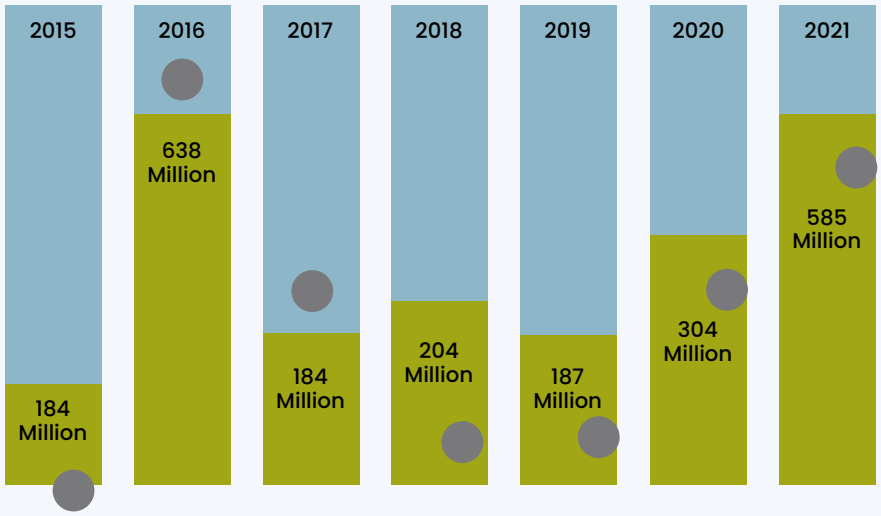


Source: Https://informationisbeautiful.net/visualizations/ransomware-attacks/

GLOBAL RANSOMWARE INDUSTRY TRENDS

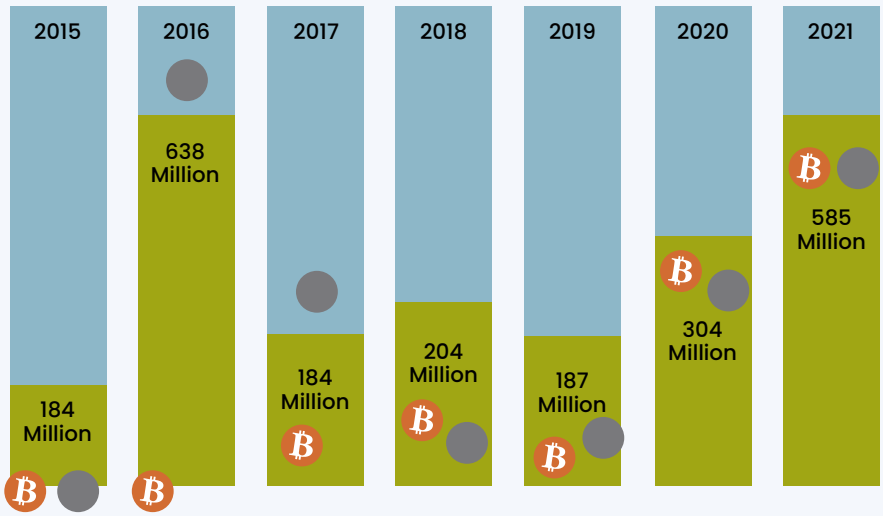


Ransomware is an ever-growing threat to thousands of organizations and businesses worldwide. Since 2016, over 4,000 ransomware attacks have happened daily in U.S. - US DOJ



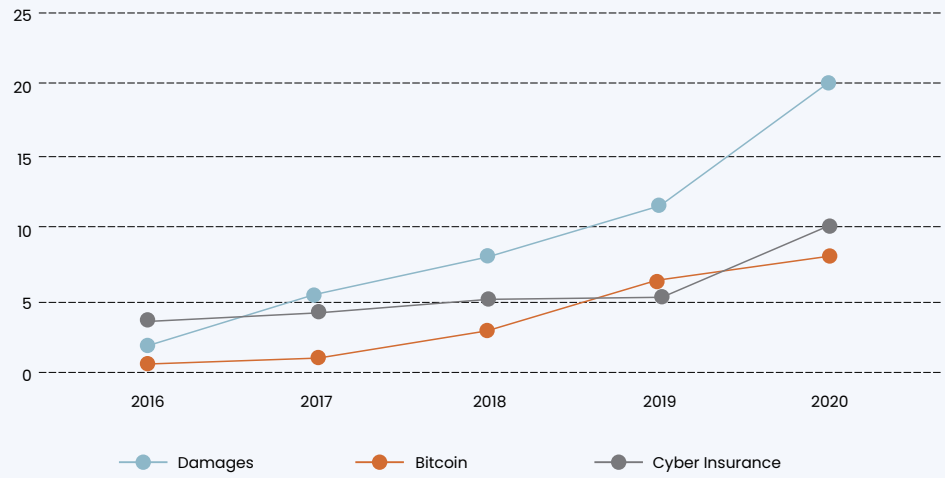
The average ransom demand made to our policyholders in the first half of 2021 was $1.2 million. That is a large price to pay for any organization, and is a nearly 170% increase from the average demand in the first half of 2020. - Coalition Cyber Insurance report 2021

GLOBAL RANSOWARE INDUSTRY TRENDS



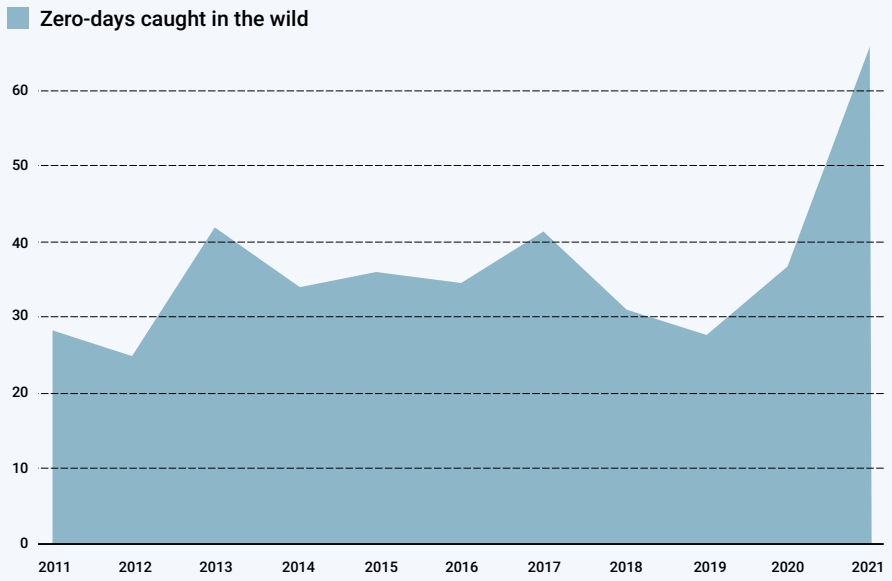
Bitcoin accounts for approximately 98% of ransomware payments. Whether an organization pays the ransom or attempts to recover the data independently, a clear understanding of bitcoin is essential for cyber incident response planning.

CORRELATION BETWEEN RANSOMWARE DAMAGES, BITCOIN AND CYBERINSURANCE



And this graphic illustrates the upward paths of each element that shows the correlation: Damages, cyber insurance, and the value of bitcoins all increased in parallel.

A BUMP UP IN ZERO-DAYS IN THE PAST YEAR



While zero-days were typically so costly that only state-sponsored groups could afford their fees, those costs have declined and now an estimated one-third of all zero-days are used by private cybercriminal organizations, according to the MIT Technology Review.

In addition, cybercriminals are now creating their own hacking tool supply chains, banding together in small clusters to extract more wealth collectively. The details are beyond the scope of this paper, but ZDNet recently published an eye-opening article showing the interconnections between threat actors. It's not a comforting picture, to say the least.

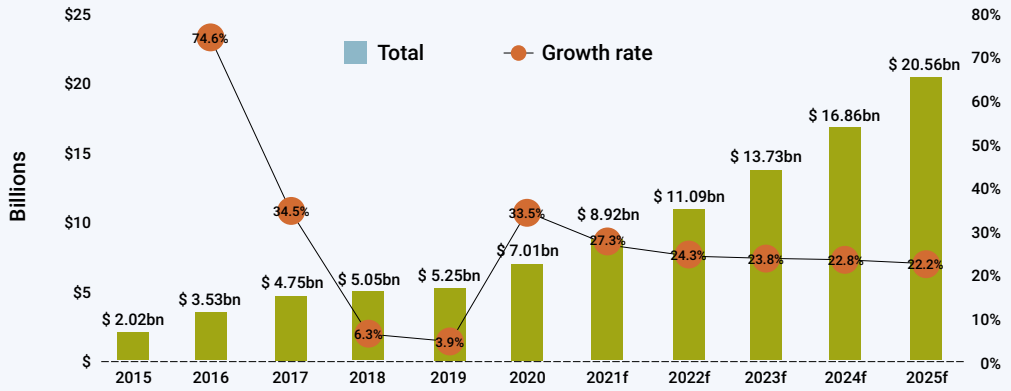
THE INSURANCE INDUSTRY STRIKES BACK… AGAINST THEIR CUSTOMERS

A 2021 study revealed that more than two-thirds (70%) of cybersecurity professionals believe insurance payouts exacerbate ransomware. The insurance industry, realizing the errors of its ways, decided it had to avoid overextending itself and losing money on its cybercrime policies. It did this two ways, according to a recent report from Dillon Behr and the RPS team in the U.S. Cyber Insurance Market Outlook.

First, carriers increased premiums and lowered coverage limits on those industry classes hit hardest by cybercrime and cyber extortion. Premiums jumped as high as 300% for companies renewing their policies from the previous year. Coverage that might have reached $5 million in earlier policies was trimmed back to a maximum of $1 million to $3 million.

Second, insurance companies insisted that the insured not leave themselves so vulnerable. They set IT infrastructure minimums, such as having MFA as an underwriting requirement. While logical, many organizations weren't prepared for the sudden change and didn't have funds set aside to beef up their security infrastructures before needing to renew their policies.

GLOBAL CYBER INSURANCE MARKET ($BN), 2015-2025F



HOW SHOULD ORGANIZATIONS RESPOND?

As noted in the beginning, there is no ready panacea for the rising threat posed by increasingly sophisticated and well-equipped cybercriminals. Certainly relying on an insurance policy for protection is not an answer anymore, and it would not be surprising to see the industry abandon coverage for cybercrimes.

Rather, it will take a coordinated effort throughout your organization to stay clear of the threat to begin with, and to respond quickly and appropriately should you be attacked. This is not an overnight endeavor. Instead, it involves a careful, deliberate review of your current status and assessment of vulnerabilities, followed by a series of well-planned investments in technology, and the training of your employees to ensure they are not inviting unwanted intrusions. Finally, you'll want to look closely at your vendors, particularly those who are supplying any software you're using, to be sure they are not exposing you to malware due to their insufficient preparations against it.

Cyber insurance is an important tool in the security tool belt because, in theory, it allows for organizations to recoup some of their financial losses incurred as a result of a successful cyberattack. What has become abundantly clear, however, is that these insurance policies should not be relied on as a compensating control to fully repair losses from a successful cyberattack. Instead, organizations need to adopt a proactive approach to security and protect critical systems against attack.

HOW ORDR CAN HELP: SEE. KNOW. SECURE.

As organizations embrace digital transformation, billions of devices are being connected to enterprise networks to facilitate operations, improve safety, and enhance operations. The promise of digital transformation can only be realized with the visibility and security of these devices – enterprise IT, IoT, medical/IoMT, and OT.

The Ordr platform was designed for this. By first seeing all devices in your environment, knowing critical data points about them, and efficiently and effectively securing them. Simply stated - See, Know, Secure.

TAKE ACTION TO MITIGATE RISK

One of the top cybersecurity requirements for any organization is an accurate asset inventory of all of the devices that are connected to the corporate network. Once all devices have been identified and inventoried, their risks can be identified; they can also be monitored and compared against a baseline of expected activity. This is done either because a certain device is already known to Ordr, or operations are established through use. Because connected devices (whether IoT, IoMT or OT) are deterministic and must operate within narrow parameters for their functions, anomalies are easier to identify. Ordr can then apply Zero Trust security policies that keep these devices on secure VLANs, communicating only with devices required for their functions, and isolated from other systems. Should an attack occur, automated policies to quarantine, block traffic or terminate a session can mitigate risks. Zero Trust policies for mission-critical systems ensure that they are kept out of harm's way, limiting an attack's "blast radius" within the connected environment.

Ordr delivers visibility and security for every connected device. The Ordr solution is agentless and SaaS-based. There is no impact to any device that we discover and secure. Within a few hours of deployment, our platform discovers every connected device, profiles behavior and risks, and automates action as described as follows:

- **See every device and network connection** – Rapid AI-powered discovery and classification of devices includes not just what the devices are at a granular level, but also what they are connected to. We deliver the complete mapping of communications for every device.
- **Know every risk, vulnerability or anomaly** – Within the Ordr Data Lake, we enrich device insights with external threat intelligence and network data to build the richest profiles for every connected device. In addition, our integrated Threat Detection Engine and Machine Learning models deliver insights into known and unknown threats, including anomalous communications that may indicate lateral movement or communications to a C2 domain.
- **Secure via automated response** – With hundreds of thousands of devices in your network, automation is critical. Ordr enables true mitigation and prevention policies across campus, data center and edge infrastructure. Once Ordr detects an exploit or a device behaving in a suspicious manner, we enforce policies to automatically contain threats through NGFW policies, ACL blocks, quarantine VLAN assignment, port shutdown, or session termination--either directly to existing firewalls, switches, wireless controllers, or via NAC platforms. These policies are all automatically generated by Ordr, and can also be enforced on existing security and networking infrastructure.

We've helped hundreds of organizations on their cybersecurity journey, and we are eager to partner with you on yours. Ordr is backed by top investors including Battery Ventures, Wing, and TenEleven Ventures. We invite you to get a demo and see how we can give you the complete protection your organization deserves.

GET DEMO