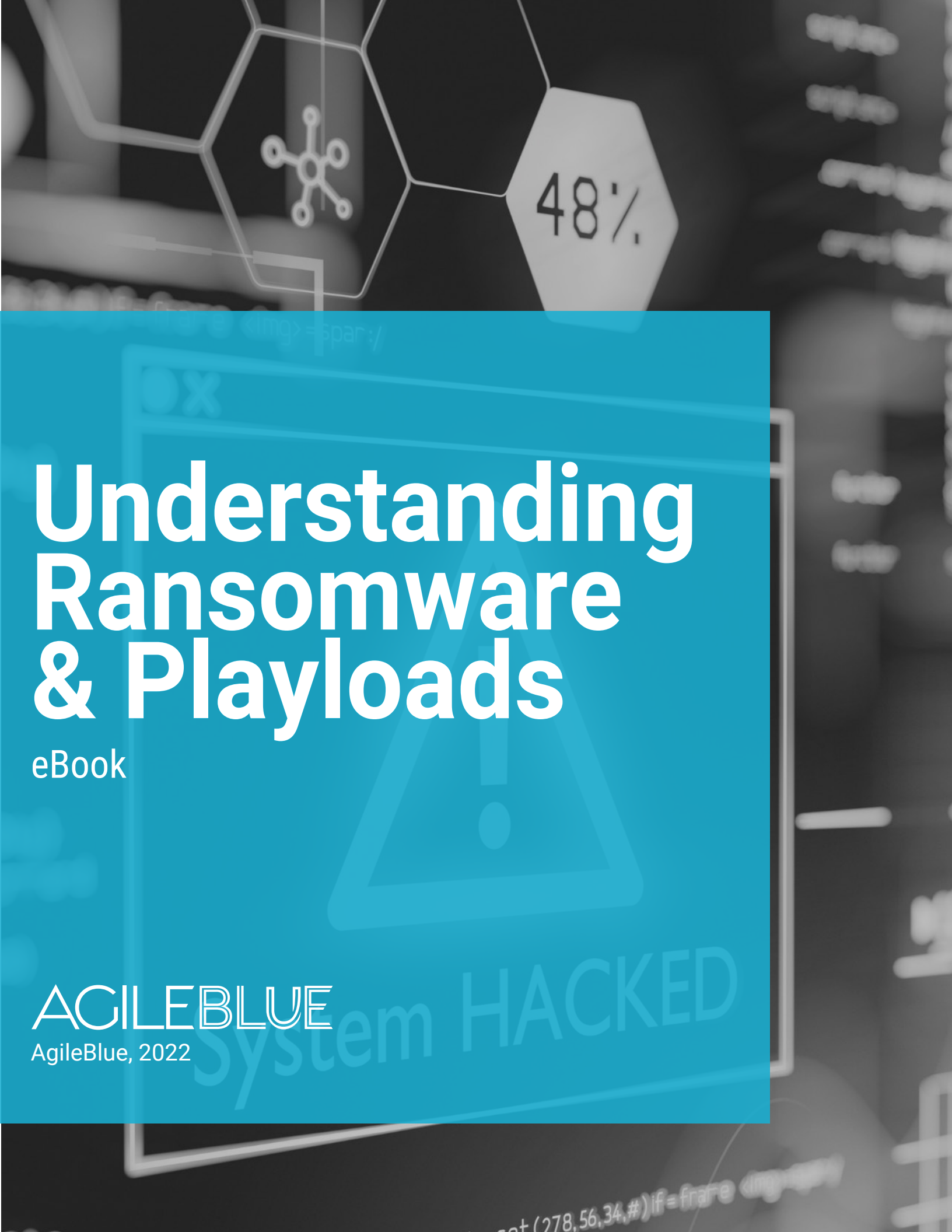


Understanding Ransomware & Playloads

eBook

AGILEBLUE

AgileBlue, 2022

What is Ransomware?

As we progress through the digital age, standard cybersecurity regulations have been forced to evolve. At one time, businesses and the public paid little to no attention to existing cyber threats. This is no longer the case, however, as technology is ever evolving; Because of this, organizations are forced to adapt. Technology, while it makes business operations happen faster, and more efficiently, it has opened a gate for new types of criminals. Before technology, business owners worried about robbing and breaking into local offices or businesses. Today, organizations are faced with a much bigger challenge: ransomware attacks.

As ransomware attackers are becoming stronger and technology continues developing, important data for businesses, state security, and even national security are at risk. In a campaign conducted by the Cybersecurity and Infrastructure Agency, U.S. Attorney General Merrick Garland and the Biden Administration have acknowledged the growing problem of ransomware and are taking action to warn businesses and the public of the ransomware threat. Not only are businesses at risk, but the federal government and states are at risk of losing critical information as well, to ransomware hackers.

How is Ransomware Used?

Ransomware is an ever-evolving form of malware that has become a significant threat to U.S. businesses and individuals during the past two years. Ransomware uses asymmetric encryption; this is cryptography that uses a pair of keys to encrypt and decrypt a file. The specific pair of keys is generated by the attacker for the victim, with the private key to decrypt the files stored on the attacker's server. Without access to the private key, it is nearly impossible to decrypt the files that are being held for ransom.

In most cases, ransomware is distributed through phishing emails, a targeted attack on an individual or organization. Once the malware has an endpoint established, it stays on the system until the goal is complete. Ransomware can easily expose system/network vulnerabilities to spread across entire organizations, and there are numerous ways to gain access to a network to encrypt data and paralyze the organization.

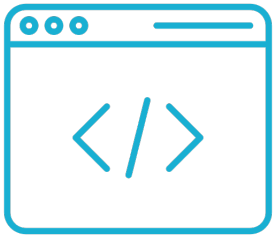
There are numerous ways to access one's network, encrypt data, and paralyze the organization. Once the files are encrypted, the end-user will be prompted to pay a ransom to get their data back from the hacker. Essentially, the hacker breaks into the network, steals the targeted data, and holds the data hostage until they receive payment. However, paying the ransom does not guarantee that you will be given all the files back as only 65% of the encrypted data was restored. Plus, paying the ransom doesn't mitigate risk of another ransomware attack.

What is Malicious Payload?

Malicious payloads are the parts of cyber-attacks which cause harm. Malicious payloads can sit dormant on a computer or network for seconds or even months before they are triggered.

These malicious payloads can come in the following forms of malware:

Disguised as a legitimate program; but uses social engineering to hide malicious code within legitimate software.



A piece of code which is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data.

Self-replicating malware that duplicates itself to spread to uninfected computers.

Software that is secretly or surreptitiously installed into a network to gather data on individuals or organizations without their knowledge

What You Need to Know About Ransomware

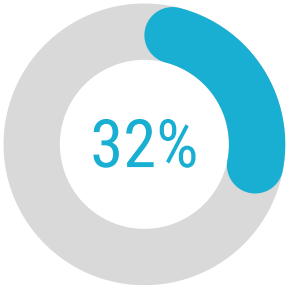
Ransomware is One of the Hardest Attacks to Defend From

According to a study conducted by Neustar, ransomware is the #1 most difficult threat to defend against and #3 on the threat priority power ranking.

Last year alone in the U.S., ransomware gangs hit more than 100 federal, state and municipal agencies, upwards of 500 health care centers, 1,680 educational institutions and untold thousands of businesses, according to the cybersecurity firm Emsisoft.

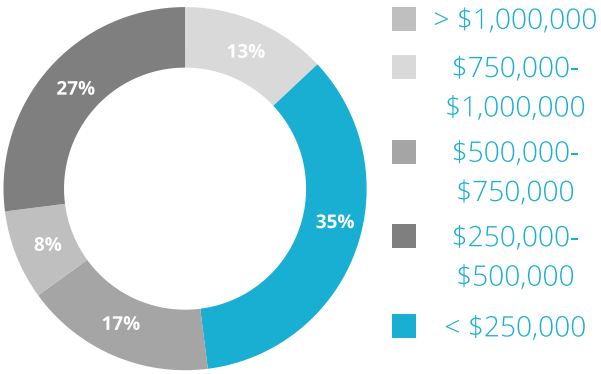
Dollar losses are in the tens of billions. Accurate numbers are elusive. Many victims shun reporting, fearing their reputation to be affected. How does ransomware work? Colonial Pipeline, JBS USA attacks explained (usatoday.com).

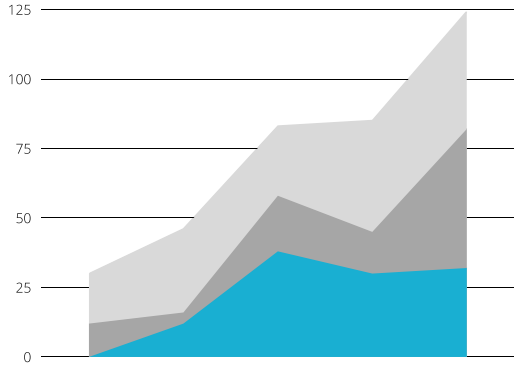
Data & Trends



Increase in Cloud-based attacks since the previous year.

Ransom Paid in 2020





Phishing Threats Rose More Than 600% in 2020

What You Need to Know About Ransomware

Ransom Payments Vary

In 2020, the average ransom payment was $170,404. However, there is a wide range that companies have paid due to ransomware attacks. In a study conducted by Sophos, it was discovered that organizations most commonly pay $10,000 in for a single attack, while 2 respondents said they have paid a ransom of $3.2 million.

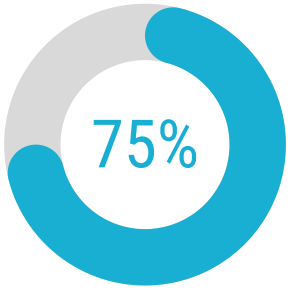
For example, last month the Colonial Pipeline experienced a ransomware attack from the DarkSide ransomware group which forced the company to pause fuel distribution on the East Coast. The group responsible infected the company's billing system in which they use to bill customers and track fuel distribution.

Wired.com reports that nearly a week after being breached, the company paid the ransom of 75 bitcoin – worth as much as $5 million. While the Colonial Pipeline was able to begin operations 5 days after paying ransom, this decision to pay will only encourage ransomware attackers to continue striking.

Note

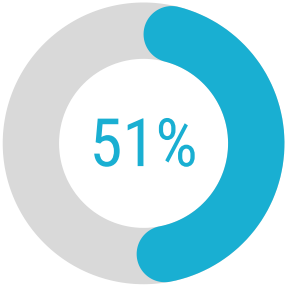
The average cost to recover from a ransomware attack has doubled since last year. In 2020, the average cost of remediation was $761,106; Today, the average cost to recuperate from a ransomware attack is $1.85 million.

Data & Trends



of IT organizations will face one more attacks by the year 2025

of all data breaches started with a phishing email internally



of malware attacks in Q3 of 2020 were ransomware attacks-up 34% from Q1

What You Need to Know About Ransomware

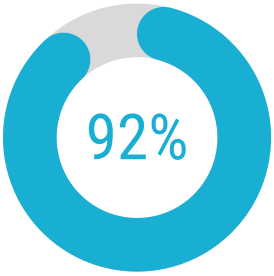
In the past 6 months, compared to 2020, companies that are paying increased by 6%. However, this doesn't mean companies are fully recovering from being breached.

Paying the ransom is an ineffective way to get organizational information back. If you decide to pay the ransom, however, keep in mind that paying the ransom could result in only 65% data restoration.

Wired.com reports that nearly a week after being breached, the company paid the ransom of 75 bitcoin – worth as much as $5 million. While the Colonial Pipeline was able to begin operations 5 days after paying ransom, this decision to pay will only encourage ransomware attackers to continue striking.

Back-up Your Back-ups

Reportedly, back-ups are the most common approach for remediating data after a ransomware attack, elect a standard method of back-ups of 3:2:1. By backing-up all organizational data, you can avoid being forced to pay ransom.



of attack victims that paid ransom failed to achieve 100% of data restoration in 2020

Actions You Can Take Today

Ransomware Prevention is the Best Defense

The key to stopping ransomware is in-depth defense that merges dedicated preventative ransomware technology and human-led threat hunting. One way to protect your organization is with a Security Operations Center as a Service (SOCaaS).

AgileBlue combines human experts and anti-ransomware technology with AgileBlue's advanced machine learning that detects attacks before they happen. We monitor every one of your cloud and endpoints faster, with a 95% true positive rate. If you don't already have the necessary skills in-house, look at recruiting support from an automated cybersecurity company that offers SOC-as-a-Service. AgileBlue detects threats before you're breached, so you can rest easy.

AGILEBLUE

AgileBlue is a software company with innovative SOC|XDR-as-a-Service for 24/7 moinitoring, cloud security, data privacy and complicnace backed by our U.S. based SOC.

We detect cyber threats before you have been breached. Our SOC-as-a-Service platform is designed to monitor your cloud, network, and endpoints. Our modern SOC-as-a-Service is built on innovative machine learning and autonomous execution. For more information, visit our website: AgileBlue.com.

Ready to start protecting your company?

Request a Demo