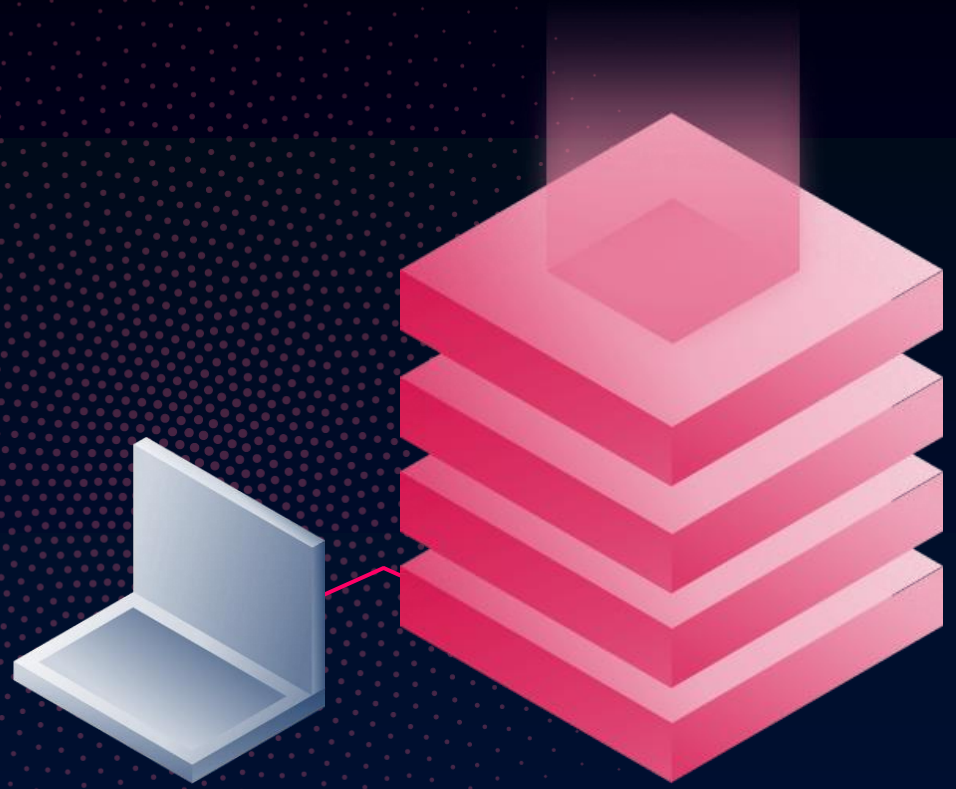
RANGEFORCE



RangeForce — eBook

Ransomware Insights

RANGEFORCE

What is ransomware?

Who hasn't heard of ransomware?

It's arguably one of the most top-of-mind topics for business leaders today. And that's not just for the cybersecurity team, but anyone who has an idea of exactly how disruptive a successful ransomware attack can be. Sadly, there's no shortage of reminders; ransomware has a tough time staying out of the headlines.

With the prevalence of this threat, it demands our attention and action. So, what exactly is ransomware?

How does it work? And what should teams be doing to stay ahead of it?

Ransomware insights

We've gathered our top ransomware insights to answer some of these questions. Read on to better understand this threat, its behavior, and steps you can take today to increase your defensive readiness against ransomware.

RANGEFORCE

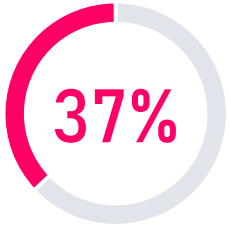
Ransomware defined

Ransomware is a specific type of malware that targets victims' valuable files and documents. It uses encryption to lock these assets, preventing victims from accessing them. As the name suggests, the perpetrators won't decrypt and release the files until a ransom is paid. Threat actors typically demand payment in some form of cryptocurrency. This is by design, and enables them to transact with increased anonymity.

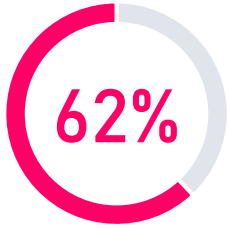
Some ransomware variants have the ability to create worst case, lose-lose scenarios. With a tactic known as double extortion, threat actors can exfiltrate their victims' data prior to encryption. This stolen data is a prized possession, and threat actors will threaten to leak it unless the ransom is paid. It's a convenient failsafe. In the event that victims do have a robust backup process in place, there's still incentive to pay the ransom in order to prevent an inevitable data leak.

RANGEFORCE

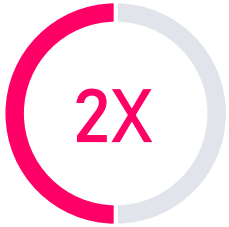
Ransomware statistics



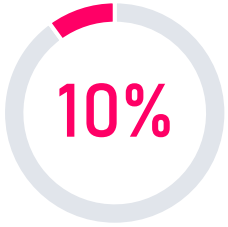
of global organizations said they were the victim of some form of ransomware attack in 2021.[1]



year-over-year increase in ransomware complaints (2,084) reported in the first half of 2021.[4]



ransomware attacks doubled in frequency in 2021.[3]



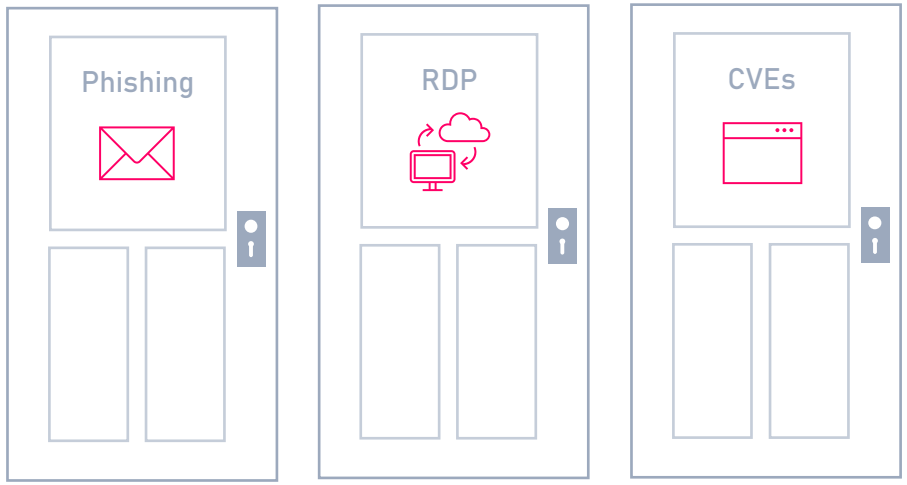
of breaches include ransomware.[2]

1. IDC 2021 Ransomware Study: Where You Are Matters!
2. Verizon 2021 Data Breach Investigations Report
3. Verizon 2021 Data Breach Investigations Report
4. https://www.cisa.gov/uscert/ncas/alerts/aa21-243a

RANGEFORCE

Ransomware access vectors

Ransomware typically uses one of three main vectors in order to gain initial access. Here's how they rank, in order of most used:



1. **Phishing**
2. **RDP**
   Public-facing RDP services
3. **CVEs**
   Common Vulnerabilities & Exposures

RANGEFORCE

Ransomware access vectors — Phishing ✉

1. Phishing

In a phishing attack, threat actors employ email-based social engineering techniques to elicit and exploit human behavior. Successful attacks will result in a user action like clicking on a malicious link, downloading an attachment, or even just opening a macro-enabled document.

Email is such a popular access vector for many ransomware variants because of its high success rate, low overhead cost, and diversity of available techniques. As it's such a ubiquitous form of communication across so many facets of day-to-day life, threat actors have near endless inspiration for creating enticing phishing lures.

How often do we think twice before clicking a link to redeem a digital gift card or download a meeting agenda?

According to Verizon Data Breach Investigations Report 2021, the amount of ransomware breaches doubled from 2020-2021, driven by large increases in misrepresentation (i.e. pretending to be someone you're not) and other social engineering tactics.

ransomware breaches doubled from 2020 - 2021.

RANGEFORCE

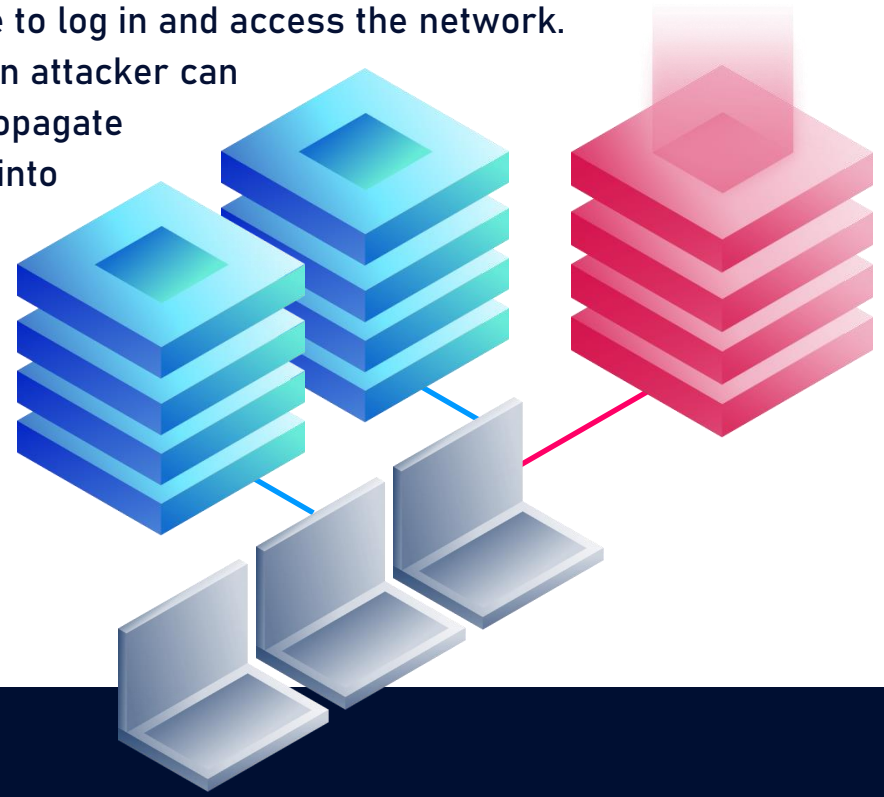
Ransomware access vectors — RDP

2. Public-facing RDP services

Any service exposed to the internet that allows a user to authenticate directly to a given system has no way to prevent unauthorized users from authenticating to the same system (threat actors included). For the convenience of remote access, many organizations leave Remote Desktop Protocol (RDP) ports open to the internet.

It's clear that the risks associated with RDP are generally underestimated. Because it uses modern encryption, RDP is acceptable for the internet. But it lacks multi-factor authentication (MFA) in its default state.

This means that any compromised credentials, successful brute force attacks, or successful password spray attack would be able to log in and access the network. From there, an attacker can attempt to propagate ransomware into the network as if they were on a VPN.



RANGEFORCE

Ransomware access vectors — CVE

6. Qualys, 2021

3. CVEs

Attackers can also leverage software vulnerabilities to infect systems with ransomware. Notable examples include Proxyshell in Microsoft Exchange and Log4Shell in the Apache web server.

There were almost 20,000 software vulnerabilities reported in 2021 alone. The good news is that software vendors have issued patches for the majority of these Common Vulnerabilities and Exposures (CVEs).

So you may be thinking, “what’s the problem?”. The problem is the very tedious job of patch management across large networks. This is difficult and time-consuming work, so much so that many organizations do not keep their systems successfully updated.

To illustrate this point, here’s a look at the top 5 CVEs used in recent ransomware attacks, according to Qualys.[6]

CVE	Ransomware Family	Patch Available from Vendor?	Date Patch was Issued:
CVE-2013-1493	Exxroute	Yes	March 2013
CVE-2013-0431	Reveton	Yes	February 2013
CVE-2012-1723	Urausy	Yes	June 2012
CVE-2019-1458	NetWalker	Yes	December 2019
CVE-2018-12808	Ryuk/Conti	Yes	August 2018

Note that none of these vulnerabilities were discovered within even the past two years. Some are nearly a decade old! And yet, they persist as common issues. Timely patching is difficult, and threat actors know this. They even actively scan for known vulnerabilities in order to identify their best targets.

RANGEFORCE

Why is ransomware so hard to stop?

Why is ransomware difficult to stop?

Ransomware is so difficult to stop in part because it fundamentally abuses normal system functions. Take encryption, for example. There's a legitimate need for businesses to encrypt files and network communications. This functionality is built into every operating system for good reason.

Anyone can be a target of ransomware.

Over the last few years, we've seen ransomware essentially take on the characteristics of its own industry entirely, with niche players and specialized variants. For example, Hades (a variant of WastedLocker) almost exclusively targets large organizations, what cybersecurity practitioners now call “big game hunting.”

Interestingly, there are some threat actors that deploy variants with a slightly more ethical modus operandi. These groups claim to avoid targeting hospitals or similar critical infrastructure. On the off chance that they do accidentally mis-strike, they'll go as far as to offer their victims free decryptors.

RANGEFORCE

To pay or not to pay: that is the question

You're probably wondering:

Is it ever a good idea to pay? Is it wrong to comply with an attacker's demands?

The answer to this question is unique to every organization. Many follow the general guidance of never paying a ransom. But the reality is that ransomware attackers are strategic and will often research an organization before setting the ransom amount. By setting the ransom's price lower than what it would cost the organization to recover from the incident on their own, attackers make an undeniable business case for complying with their demands.

Another point of consideration: ironic as it might be, ransomware groups have an incentive to make true on their promises and protect their reputations. If a ransomware group is known to reliably release data after payment is made, it puts itself in a better position to continue operating and collect future ransoms.

However, it's important to keep in mind the recommendations of government agencies like the FBI, which publicly cautions against paying a ransom

RANGEFORCE

To pay or not to pay: that is the question

"The FBI does not advocate paying a ransom, in part because it does not guarantee an organization will regain access to its data. In some cases, victims who paid a ransom were never provided with decryption keys. In addition, due to flaws in the encryption algorithms of certain malware variants, victims may not be able to recover some or all of their data even with a valid decryption key.

Paying ransoms emboldens criminals to target other organizations and provides an alluring and lucrative enterprise to other criminals. However, the FBI understands that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers."

— Federal Bureau of Intelligence (FBI) PSA,
High-Impact Ransomware Attacks Threaten U.S. Businesses And Organizations

In any case, the growing threat of ransomware has provoked many organizations to proactively craft payment policies. That being said, there are still critical factors to consider when deciding whether or not to pay. As with any security-related issue, the threat of ransomware demands careful risk analysis. Regardless of how your organization chooses to respond, the following cannot be overstated:

> The time to develop a ransomware payment policy is not during an attack; it's before.

If your organization hasn't resolved this yet, the time to do so is now.

RANGEFORCE

How to stop ransomware

An organization's best chance against ransomware is a robust cyber defense readiness strategy that can prevent an attack or contain it at its onset. Unfortunately, with the variety of initial access vectors and diversity of techniques, there's just no magic bullet.

Ransomware's infamous file encryption typically happens near the end of the attack chain. As such, an organization's best defense is disrupting an attack early in its sequence. Once a cyber adversary reaches the point of encryption, the best you can hope for is containment.

The worst examples of ransomware breaches largely resulted from poor security postures in the first place. If more robust patch management or network segmentation had been implemented, the damage could have been significantly reduced.

Successful mitigation in three primary areas can help prevent initial infections:

- People-related security: security awareness, email security controls, and endpoint security
- Attack surface reduction (i.e. application and filetype allow lists)
- Aggressive vulnerability management for public-facing assets

But even with the above tactics in place, it's very possible that sophisticated ransomware could still gain entry. With this in mind, containing the threat becomes your next highest priority. Mitigation efforts at this stage include:

- Network segmentation to protect assets with different vulnerability management lifecycles
- Credential management on active directory and other systems to prevent spread with compromised credentials

RANGEFORCE

How to stop ransomware

It's also crucial to have the right tools for the job. So what are they? Different solutions each help in unique ways. A security stack best prepared for ransomware incidents should include the following capabilities:

- SOAR: Automated workflows reduce mean-time-to-detect and mean-time-to-respond to assist disruption and containment of breakthrough malware.
- Next-Generation Firewall (NGFW): Advanced analysis of network traffic and downloaded objects can detect known strains of malware through signatures and heuristics.
- Secure Web Gateway (SWG): Deep visibility into internet-bound traffic can uncover known malware samples and command and control (C2) traffic.
- Endpoint Detection and Response/Endpoint Antivirus: Signature-based endpoint detection is critical for stopping known threats and application execution control can stop emergent malware.

RANGEFORCE

Top 5 ransomware protection security controls

Ultimately, there are specific security controls that will bolster any organization's readiness against the threat of ransomware considering the areas of vulnerability that we've discussed. Here are the top five according to our team:

1. Security Architecture: Network segmentation and micro-segmentation help to contain threats if and when they break out in a given zone
2. Identity and Access Management: Incorporating Least Privilege and Zero Trust principles into your Identity and Access Management (IAM) plan are crucial to mitigate the spread of ransomware. Multi-factor authentication can also serve to mitigate attacks in the event of account compromise. These efforts reduce the attack surface thus limiting unauthorised access.
3. Threat Intelligence: The use of a Threat Intelligence Platform (TIP)–or at the very least a threat intel feed–can aid security teams in proactively defending against ransomware by providing real-time information on current threats. TIPs have the added advantage of automation and machine learning capabilities to assist incident response strategies.

RANGEFORCE

Top 5 ransomware protection security controls

5. Security Awareness: The largest access vector of ransomware is phishing, which we can fundamentally attribute to human behaviour. Continuous security awareness training across the organization is vital to stopping this front line threat. Internal phishing campaigns and interactive training are excellent ways to teach staff to identify and report potentially malicious emails.

6. Continuous Cyber Skill Development: Consider a situation in which a security protocol correctly identifies and escalates a threat, but the personnel lack the skills needed to handle it. It's hard to imagine a more frustrating or destructive scenario for everyone involved. For this reason, it's crucial for security professionals to see the latest threats in controlled environments where they can learn to successfully identify and respond to real-world situations. Hands-on exposure ensures that your security control investments are properly put to use. By continuously honing skills, your team can make sense of obscure alerts, correctly triaging and responding to threats before your organization becomes the next victim.

About

RangeForce empowers cyber readiness at scale.

Refine individual and team capabilities against the latest threats with a continuous approach to cybersecurity skills development. See real threats in action and sharpen the skills needed to defend your organization with interactive modules, challenges, and team-based threat exercises that reflect the real world.

Learn more →