REDSEAL

Ransomware 2.0

What your business needs to avoid compromise in the cloud

Introduction: Ransomware is changing

Ransomware has a longer history than many of us realize. In fact it can be traced back over three decades to the floppy disk-based AIDS trojan. The concept is simple: make the data on a victim's computer or network unavailable and then charge them a ransom to regain access.

The threat we know today is really the product of several interweaving trends: technological innovation, digital transformation and geopolitical reality. Advances in cryptocurrency enabled threat actors to monetize their efforts while remaining anonymous. And further tech innovation led to the development of powerful malware capable of encrypting multiple file types at speed and scale. Some ransomware variants can now scramble 100,000 files in as little as four minutes. As organizations invested in digital technologies over the course of the past few years, especially during the pandemic, their cyber-attack surfaces also grew. In effect, this made them a bigger target for adversaries.

Some ransomware variants can now scramble

100,000 files

in as little as four minutes.

The criminal market has continued to evolve, including the emergence of affiliate groups and ransomware-as-a-service (RaaS) offerings on the cybercrime underground. RaaS has streamlined the management and deployment of ransomware attacks in a SaaS-like way, so that even actors less technically proficient can share in the spoils. They operate with impunity from hostile states like Russia, shielded from law enforcement as long as their targets align with the government's geopolitical foes.

But ransomware is changing. Target organizations have learned to back up data regularly and store it in the cloud in response to the first wave of basic ransomware attacks. What does this mean? That the arms race between attackers and defenders continues to evolve, forcing the offensive team to adapt its tactics. So where once a ransomware payload was enough to extort payment, now data theft and exfiltration are also used. Where once the path of least resistance was a distracted user and a phishing link, now threat actors are being forced to probe cloud environments for entry points to exploit.

This is the new reality of Ransomware 2.0. It follows that mitigation will require a much greater effort than before—to map on-premises and cloud assets, and understand and control network paths to and from these assets. The good news is that RedSeal can help with both.

Why should you care about ransomware?

There's a reason why everyone's talking about ransomware. Over the course of 2021, attacks rocked the US and beyond, disrupting everything from major oil pipelines to complex food supply chains. And these were just the "big-game hunting" attacks that hit the headlines. In reality, no organization or vertical is safe.

SMEs comprise the majority of overall targets. One estimate put the number of attempted attacks in 2021 at 650 million, a 105% year-on-year increase. Yet even this is based on the data of just one vendor. The real scale of ransomware threats is likely to be far larger. In the UK, the NCSC security agency describes ransomware as the number one threat facing SMEs and enterprises.

It's estimated that the ransom payment itself could be as little as 15% of the total cost of a ransomware compromise. That makes the threat a critical business risk that should command boardroom-level attention in any organization.

As of Q1 2022, the average ransom stood at just shy of **$212,000**. But that's only one of many Ransomware 2.0 "costs" that organizations need to consider. The financial and reputational impact of service outages and data breaches could include:

- Regulatory fines
- Reputational damage
- Legal costs (e.g. from class action lawsuits)
- Customer churn
- A slump in share price
- IT overtime
- Productivity losses
- Lost sales
- Business disruption
- Third-party forensics/investigation costs

What is Ransomware 2.0?

Things used to be much simpler. There was a period of several years beginning with the emergence of CryptoLocker when cryptographic ransomware followed a predictable pattern.

1) **Threat actors would gain initial access** to environments via one of three key vectors:
   - Phishing emails – designed to covertly install software on the victim's machine.
   - Vulnerability exploits – increasingly leveraged by cybercrime specialists known as initial access brokers (IABs), who sell access to other groups.
   - Remote desktop protocol (RDP) abuse – the exploitation of unpatched or misconfigured RDP servers. These are often left protected only by weak or previously breached credentials.
2) **Attackers would pivot from initial access** to find business critical resources. This lateral movement primarily occurred on-premises, where most sensitive corporate data was stored.
3) **The threat group encrypted sensitive data and** sent a ransom note.

Now things are changing, as organizations get better at following security best practices (i.e. taking regular backups) and digital transformation means more data is stored in the cloud. This has led to the emergence of two key trends:

I – Data theft, exfiltration, and leakage

As more organizations backed up their data, fewer were paying the ransom, choosing instead to endure several days of operational outage and pain to restore from backups. But the cybercrime economy is alert to changing trends and quick to adapt. Thus was born the concept of "double extortion" or "double dip" attacks. That is, before encrypting data, attackers will exfiltrate what they can to an external server under their control.

This data could include personally identifiable information (PII) on customers and employees which may have a significant regulatory compliance and reputational impact. It could even be sensitive IP, potentially putting competitive advantage at risk.

The exfiltrated data is typically put on a dark web "blog" or leak site. Initially a taster sample is published, with victim organizations told they have a short window in which to pay up, or else the entire trove will be leaked or sold. In reality, once data has been obtained, there is little incentive for the threat group not to monetize it, even if their victim pays up.

To pile on the pressure, many ransomware groups now also:

- Send extortion emails to corporate users, demanding payment or else they'll leak everything
- Call up employees, customer and/or partners urging payment
- Create a dedicated surface web site for each victim, searchable by any customers/employees to see if their data has been compromised

Exfiltration is the new normal: 77% of ransomware cases analyzed in Q1 2022 followed this pattern. Some attacks eschew encryption altogether to focus on data theft as the sole means of extortion.

II – Ransomware in the cloud

The days when threat actors could limit attacks to the on-premises corporate network are largely over. Organizations increasingly do business in the cloud. One 2021 report predicted that within 12 months, 54% of enterprise workloads would reside in the public cloud. If ransomware actors therefore want to lock down business-critical systems and steal sensitive data, it is increasingly to the cloud they must turn.

Fortunately for them, and unfortunately for many organizations, there are plenty of opportunities to achieve both initial access into cloud data stores and lateral movement from on-premises networks. Why? Because IT teams regularly misconfigure their cloud environments. Some typical examples include:

- Configuring AWS S3 buckets to be "world readable"
- Misconfigured VPC/VNET security groups
- Kubernetes policy mistakes

The challenge for IT security leaders is that there simply aren't enough skilled engineers in most organizations to understand and manage cloud environments securely.

The problem is exacerbated by:

- Continuous cloud innovation from the big platform providers—adding more features, creating greater complexity, and ensuring there are more ways to get things wrong
- Environments composed of different cloud platforms, which multiply this complexity: 92% of enterprises are estimated to have a multi-cloud strategy today

What does this mean?

Cloud misconfigurations like this have led to the accidental leakage of billions of sensitive records over recent years. However, in most cases, they are discovered first and responsibly disclosed by security researchers. The difference with ransomware is that threat actors are actively scanning for these configuration gaps. Like a burglar twisting doorknobs on the houses on a block, they'll keep on trying until they find one unlocked.

All of this probing can be done anonymously, remotely and with automated tooling. It provides access to sensitive data stores for exfiltration and encryption, and enables further lateral movement to other cloud assets. In short, attackers are becoming more agile, and so too must defenders.

Beyond benchmarks: how to mitigate Ransomware 2.0

These combined trends will require a more proactive approach than the one used to tackle legacy ransomware attacks. It's no longer enough to have backups and/or follow CIS benchmarks for best practice security —organizations must prevent exfiltration and control inbound, outbound and internal traffic in their cloud environments.

This requires first gaining holistic visibility into all network and cloud assets, and then understanding all network paths to and from these assets—no matter which combination of cloud providers you're using. This is the value RedSeal delivers. We empower customers to:

- Continually discover all their network and cloud assets – this is particularly important in the cloud, where assets are dynamic and ephemeral
- Continually understand the configuration status of these assets – so customers can take action to remediate/secure them
- Map all connectivity within and between clouds and on-premises networks
- Build segmentation policies to restrict data exfiltration and unauthorized cloud access/lateral movement
- Continually monitor and remediate any policy compliance drift

Modern, cloud-centric organizations are characterized by complexity. It is this complexity that ransomware actors are exploiting through automated tools. Every pathway, every credential and every storage bucket must be correctly configured. Miss just one detail, and there's a good chance they will find and monetize it through ransomware and/or data exfiltration.

Here's how we can help you

RedSeal sees what your scattered DevOps teams cannot. We spot these security and configuration gaps before the bad guys do, to get customers one step ahead of Ransomware 2.0. No other platform has deep situational awareness of all your network environments—public cloud, private cloud and physical. Not just identified points, but the connectivity between them. RedSeal's cloud security solution takes an organization's awareness of its network infrastructure and translates that into actionable priorities. Alongside this, we augment customers' security teams, making network situational awareness more widely available, and helping customers increase their digital resilience.

Organizations will get better at defending against traditional threat techniques and policing access vectors like email phishing, vulnerability exploits and RDP compromise. This in turn will accelerate the arms race to make cloud misconfigurations an increasingly critical battleground for potential compromise. You can't fight the next war using the tactics from the last one, and equally, you can't protect what you can't see. RedSeal provides visibility and control where you need it to mitigate the risk of Ransomware 2.0.

ABOUT REDSEAL (redseal.net)

RedSeal — a security solutions and professional services company – helps government agencies and Global 2000 companies see and secure their on-premise networks and cloud environments. RedSeal Stratus, the company's SaaS CSPM solution, gives an integrated view of cloud security posture through visualization of cloud-native and Kubernetes controls, and shows which resources are unintentionally exposed to the Internet. RedSeal's Classic product brings in all network environments – public and private clouds as well as on-premises. This award-winning security solution verifies that networks align with security best practices, validates network segmentation policies, and continuously monitors compliance with policies and regulations. It also prioritizes mitigation based on each vulnerability's associated risk. The company is based in San Jose, California.

REDSEAL

+1 408 641 2200 | 888 845 8169 | redseal.net | info@redseal.net