REDSEAL

All Grown Up: The Rise of Ransomware 2.0

In 2021 there was a

62% increase

in attach volumes reported to the FBI's Internet Crime Complaint Center compared to 2020

In the first six months of 2021, the FBI's Internet Crime Complaint Center (IC3) received 2,084 ransomware complaints. Reported losses totaled over $16.8 million, representing a 62 percent increase in attack volumes and a 20 percent increase in costs compared to 2020. And over the course of 2021, 37 percent of organizations said they were victimized by some form of ransomware.

Sadly, this isn't surprising news: Attackers recognize the value of stored data and have seen sustained success with ransomware efforts, so it only makes sense that they're leaning into this approach as enterprises generate, store, and use more data across local and cloud-based services.

Defenders, meanwhile, are getting wise to more familiar ransomware tactics, such as the use of malicious email attachments or redirects to compromised websites that download and install malware packages. Companies have also gotten better at regularly backing up machines on their network, in effect taking the sting out of traditional ransomware since they can simply repopulate devices using recent recovery images.

The result of better responses, however, is an arms race. Recognizing that existing attacks are starting to stall out, malicious actors are now putting in the time and effort to create new ransomware approaches that are more sophisticated, more aggressive, and more capable of finding and capturing valuable data where it lives. This is exacerbated by the rapid adoption of hybrid work, which sees staff splitting their time between secure corporate networks and not-so-secure home offices. Add in the fact that 50 percent of organizations now plan to store sensitive data in the cloud, and attackers are reimagining familiar processes to make best use of new IT environments.

This is the rise of ransomware 2.0. Here's what it means for your organization — and how you can fight back against new attack efforts.

This Isn’t Your Father’s Ransomware

Attackers are evolving.

It makes sense: As network defenses improve, ransomware 1.0 isn’t seeing the same success. Companies are familiar — almost comfortable — with version 1.0 because it follows standard formats and prompts straightforward responses.

For example, when staff think of ransomware, they often think of large volumes of spam emails sent to corporate addresses in the hopes that someone will click through and download a malware package. Not only have firewalls and filters improved to the point where they can often detect these spam emails, but many companies have intrusion detection services in place that prevent users from opening potentially malicious attachments. As a result, it’s easy for companies to get complacent and assume that ransomware is effectively a solved problem rather than a constantly-changing landscape.

It comes down to a simple (if not so pleasant) truth: All efforts at security develop an ecosystem of thieves — ransomware is simply the latest iteration. Bolstered by easy connections with like-minded individuals, ransomware groups are getting more organized. They’re working together to overcome security controls and defeat active detection methods because, for them, there’s no downside to parallel problem-solving. If one attacker manages to circumvent a protective device, it’s worth sharing this information with the community at large to see what other avenues can be exploited.

Organizations, meanwhile, are often more reticent to share information about potential security breaches since this disclosure could have negative impacts on both reputation and revenue.

Put simply, this isn’t your father’s ransomware. This is a new day, a new dawn, and a new approach to network compromise.

Exploring the New Threat Landscape

Ransomware 2.0 has rapidly become an endemic issue as attackers find new ways to infiltrate networks and gain access to critical data. While this comes with a host of evolving attack vectors, three, in particular, represent a rapid rise in risk: Ransomware-as-a-service (RaaS), double extortion, and cloud-based attacks (also called random cloud).

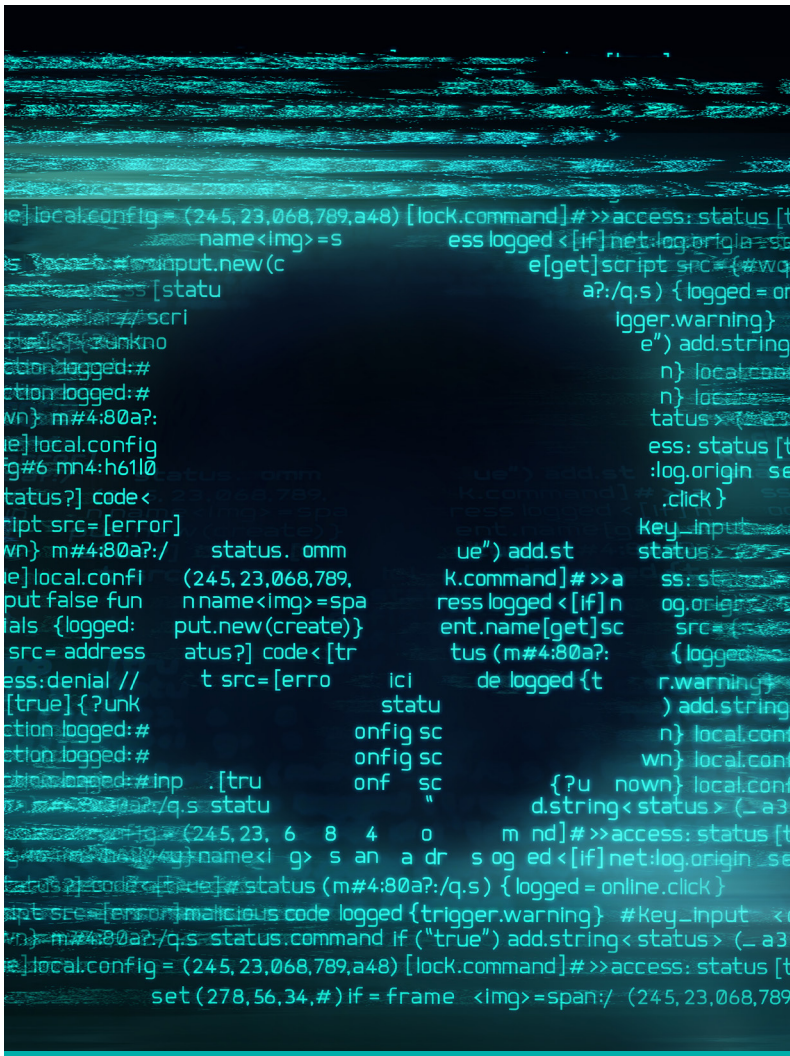
Here's a look at each.

Ransomware-as-a-Service (RaaS)

RaaS focuses on the development of ransomware packages that act as middleware. Highly-skilled ransomware designers build new tools using the latest exploits and exfiltration frameworks and then sell these tools to would-be attackers with low (or no) skill in coding but who are willing to spend money on reliable ransomware packages.

In effect, ransomware designers are taking the easy road by creating an ecosystem of RaaS sales to create an economically-viable operation. They charge users a fee for service and, in many cases, even provide "customer support" if users can't figure out how to effectively deploy ransomware tools or if they run into unexpected challenges. This creates an economy of scale scenario where it makes more sense for attackers to scale up and out for maximum profit.

RaaS also boasts an impressive cycle time. Since high-level attackers are only responsible for creating new packages, they can devote nearly all their time to research and development while buyers make best use of frameworks that they've purchased. And by continually sharing data about what works and what doesn't, RaaS vendors can improve the next generation of ransomware payloads to be less noisy, more effective, and even better at encrypting key data.



Double Extortion

Double extortion is the practice of first locking down corporate data and then threatening to release this data to the public or sell it for profit if ransom demands are met.

This is a significant change from the original ransomware model, which saw attackers encrypting data and threatening destruction if they weren't paid on time. While this was potentially damaging to businesses, it became less concerning as data backups improved and cloud-based services became available — even if attackers gained a foothold, companies could just restore data access from recent backups and ignore the ransom request.

As compliance regulations and public scrutiny of business practices have evolved, however, attackers realized that a double-extortion approach provided more leverage for ransom requests. If they could effectively exfiltrate and then encrypt data, simply restoring from backups wouldn't solve the problem for companies. Instead, the risk of having secure data exposed is now used as leverage to convince companies that they're better off paying the ransom. This double extortion approach is especially effective against companies that store personal, financial, or health information that is highly regulated under state or federal laws since the loss and/or publication of this data could lead to significant fiscal and functional consequences.

Cloud-Based Attacks

Attackers are also looking to the cloud for new opportunities. Why? Because in the cloud, there's no one to click the link. While this seems like a potential security benefit — after all, employees are often the biggest risk to corporate IT security — it also gives attackers the opportunity to explore cloud environments at their leisure.

Increasing complexity is also driving greater ransomware 2.0 risk. As companies shift more and more of their services and solutions off-site — from storage and compute to analytics and automation — networks become both larger and more complex. What's more, they lose one of the most important features of "traditional" IT operations: Perimeters.

Historically, perimeters defined secure network spaces. Anything attempting to get past the perimeter required vetting and authentication, while users inside the network could rest easy that data and processes were secure. The uptick of cloud, mobile and IoT-connected technologies, however, has created a perimeter-less environment that makes it possible for attacks to come from any direction at any time.

For malicious actors, this flips the script. Rather than trying to trick users with spam emails or fake websites, they're skulking about on cloud networks, trying every door and window they can find. If they discover one open, they simply climb inside and start looking for ways to move deeper into business networks and lock down key data.

Fighting Ransomware 2.0

The key to fighting ransomware 2.0 lies in the ability to understand and visualize the difference between traffic patterns and traffic pathways, backed by a plan to reduce the risk of lateral movements and data exfiltration.

Tackling Traffic

Think of it like this: Pathways exist across your entire network superstructure, from local servers to cloud-based stacks to mobile devices. Traffic — both benign and malicious — moves across these pathways to reach its destination. This could take the form of an employee requesting legitimate access to a service or solution and backing it up with proper authentication, or it could be an attacker attempting to circumvent network defenses. In both cases, understanding traffic patterns can help companies identify potential risks.

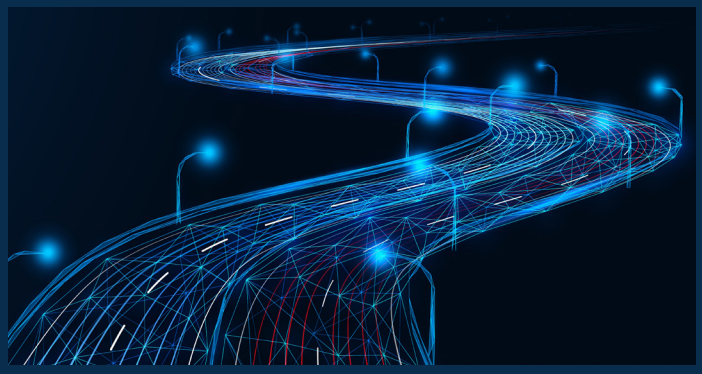
But this is only half the battle. To effectively reduce the risk of successful ransomware attacks, you need complete visibility of all potential traffic pathways. Consider the cloud. The distributed nature of cloud services means that there could be dozens — or hundreds — of pathways to and from critical services or protected data repositories. While these pathways may not currently contain any traffic, attackers could leverage them to access unknown weak points or vulnerabilities.

To put it another way: What you can't see can hurt you. By proactively mapping out pathways across your network, you can determine which routes are most commonly used and secure, which present low-probability risk, and which represent a compromise waiting to happen. Tackling and tracking traffic routes before problems occur is one of the best ways to spot threats before they become big problems.

Minimizing Movement

It's also critical to consider the role of movement across your organization.

Here's why. Traditionally, companies have been cautious about incoming traffic. To protect networks from possible compromise, they leveraged security perimeters that allowed virtually no traffic in but let almost everything out. Since enterprises couldn't verify the source of incoming traffic, denying access permissions until



basic analysis could be carried out and eventual whitelisting was completed only made sense. When it came to outbound traffic, however, policies were more permissive. Employees needed access to public-facing Internet services, so once they were authenticated on the network, there was little to stand in their way.

In the landscape of ransomware 2.0, however, this outbound approach becomes problematic. If attackers manage to gain entry, they're effectively home-free. Once they find data they want to encrypt and exfiltrate, getting it off the network requires no additional effort. As a result, companies must consider the potential threats that are coming from inside the house. For example, if executive accounts are compromised, what permissions do they have to access, copy and send data? What checks and balances exist to ensure these data operations are assessed — and terminated — if necessary?

There's also a growing need to consider the impact of lateral network movements, especially in the wake of IoT adoption. While Internet-connected sensors and devices offer the benefit of new data streams and added operational insight, they often present an ideal route for attackers to infiltrate networks undetected. In part, this stems from the limited (or absent) nature of firmware security on devices, and in part, it's tied to the pervasive sense that these devices present a lower security risk. While this is true if there was no way for attackers to shift sideways into more extensive networks, real-world attacks have shown that IoT networks are a common point of compromise.

The Real Deal: Addressing the Reality of Ransomware 2.0

While attackers haven't entirely given up on ransomware 1.0 efforts such as familiar phishing attacks and brute-force account compromises, the evolving nature of IT defense coupled with the ongoing shift to hybrid work has encouraged evolution among attacker groups. From creating RaaS efforts driven by economies of scale to the adoption of double extortion for more significant attack impact to targeting open doors and windows in the cloud, malicious actors are working hard to stay ahead of security best practices.

The bad news? There's no silver bullet. No single service or solution that will fully protect networks from ransomware 2.0. The good news? By addressing common sources of concern, such as increasingly complex traffic pathways and overly permissive network movements, companies can improve their chances of early detection and reduce the risk of ransomware 2.0 compromise.

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