Ransomware 3.0

Can Now Infiltrate Immutable and Air-Gapped Backups

asigra

According to a recent report by the NCC Group, ransomware incidents surged from 121 in January 2022 to 185 in February 2022, roughly registering a 52.89% growth in ransomware attacks between January and February 2022. This is a worrisome trend because the high spike came during months where ransomware activities have traditionally been on the lower side.

Ransomware payouts have surged astronomically as well. In 2016 the total tracked ransomware payouts were roughly $24M but by 2021 they exploded to over $600M. The average payout is estimated to be $322K in the final 3 months of 2021. The global damage from ransomware is much higher than payouts, estimated to be around $20B today and could grow to $265B by 2031.

We are currently witnessing an enormous surge in both the number of victims and an increase in the average size of payouts of ransomware attacks. While there are many factors driving this adverse trend, part of ransomware's resurgence can be traced to the emergence of Ransomware 3.0 and the golden opportunity handed to hackers by companies shifting to remote work infrastructures nearly overnight in the wake of the pandemic.

What is Ransomware 3.0?

Ransomware attacks are often distributed using trojans, phishing and exploiting unsecured Remote Desktop Protocols (RDPs). Once the criminals gain access, they typically leverage a combination of malware, open-source penetration testing tools, and living-off-the-land techniques to break down each access barrier and move laterally across the network. When they manage to gain the desired level of access, they can easily target mission-critical data for exfiltration and encryption.

And all of those are just techniques we have witnessed in the first (and now, dated) wave of ransomware.

Enter Ransomware 3.0.

Ransomware 3.0 marks the rise of a new era for a whole new breed of ransomware. This is Ransomware at scale. Ransomware 3.0 is enabled by the proliferation and increased convenience of ransomware tools, a level of sophistication in attack strategies rarely witnessed before, and a change in criminal enterprise strategy. Instead of conducting attacks individually, large ransomware organizations have consolidated into an oligarchy that enables hackers with varying ranges of skill sets to successfully carry out individual hacking ventures.

This strategy of expansion has exponentially increased the threat and risk to companies worldwide. Ransomware is now a multibillion-dollar industry that needs to grow through positive revenue traction annually. In an effort to improve profit margins, attacks are now expanding to new markets such as Cloud SaaS services. Ransomware 3.0 attack breeds are capable of spreading to the cloud and encrypting the critical SaaS data of cloud services. With more sophisticated algorithms released each year, attack strategies are changing drastically from one year to the next. With each iteration, the attacks become more proficient at spreading more easily across networks. We now have ransomware capable of deactivating on-premise antiviruses and backup agents and deleting or infecting secure backups.

The simple reason behind the growth of ransomware payouts

Ransomware is growing because hackers are getting the ransoms they ask for. From a business owner's perspective, it is simply logical to pay out than risk the indescribable damage wrought by the attacks. Doing so encourages the hackers to continue attacking other companies and opens the victim up to repeat attacks.

Historical data shows us that the trend toward organization started around 2016 and moved from individual attacks to ransomware tool distribution at scale. The trend eventually morphed into the current variation of ransomware-as-a-service (RaaS). Under this service model, major groups take the responsibility of outfitting hackers with all the necessary tools and knowledge required for carrying out the attacks. The hackers themselves could be a motley group with

varying levels of expertise including novice attackers with limited proficiency. Once the attack is carried out and the payout secured, the hackers can pay out a percentage of the profits to the ransomware group or developers.

The three major ransomware groups active currently are LockBit 3.0, Conti, and BlackCat. Recent data indicate that each of them was responsible for 42.2%, 17.8%, and 11.4% of recorded attacks respectively. Needless to say, hackers have been particularly adept at adaptation and secured enormous payouts from a variety of targeted industries and businesses. In such a scenario, organizations will need to **learn and adapt their strategies** as well.

Understanding the Expansion of Ransomware Criminal Strategy

Ransomware-as-a-Service Gangs

Potential criminals can also make use of Ransomware-as-a-service (RaaS) with a subscription-based model. Once affiliated, hackers can use 'plug-and-play' ransomware tools to execute ransomware attacks. Affiliates earn attractive percentages from each successful ransom payment. This removes the relatively high cost of entry barrier of technical competence in coding (that hitherto limited the number of truly successful hackers) and makes ransomware accessible to all, including hackers with limited capacities and experience.

Ransomware as a Service (RaaS) is a successful adaptation of the Software as a Service (SaaS) business model. Like SaaS solutions, the tool enables any user to proficiently wield the tool without functional knowledge of the technical framework. RaaS solutions enable the execution of highly sophisticated cyberattacks. Successful payout results in very high dividends for the affiliates. Recent data indicates that some affiliates earn as much as 80% on successful payouts. This results in a very high earning potential for little effort and a low barrier of entry, resulting in a proliferation of both affiliates and victims.

The Business Model of RaaS

- A business model that leverages economies of scale with a higher incidence of attacks as ransomware gangs rent out their 'plug-and-play' software to affiliates that subscribe or/ and pay back a percentage of the payout to the gang
- Enables hackers to carry out sophisticated attacks with low levels of technical literacy
- Easy to access on the dark web
- 24/7 customer support, user reviews, and forums
- Attractive payout and success rates have allowed ransomware gangs to proliferate and rapidly increase the number of affiliates

The RaaS model works because RaaS developers work to build software that enables a high chance of penetration success with a low chance of discovery. The 'plug-and-play' code is adapted to a multi-end user infrastructure. Ransomware affiliates are provided with tutorials and onboarding documentation with step-by-step guides to launch attacks. More advanced solutions equip affiliates with a centralized dashboard that can monitor the status of simultaneous attacks. RaaS groups recruit affiliates at scale with forum posts on the dark web. There is prestige associated with gaining entry into more elite ransomware gangs, like Circus Spider, that only takes in affiliates with a predetermined list of technical skill sets.

The shift of focus towards SMBs, healthcare and public departments

Ransomware attacks are on track to become the fastest-growing cyber security threat targeting small to mid-sized businesses (SMBs). Datto's 2020 State of the Channel Report showed that 70% of managed services providers (MSPs) reported ransomware as the most common malware threat to SMBs. Smaller businesses are ripe for the taking as they often lack awareness, budgets and access to updated defensive tools and strategies. For hackers, SMBs form the 'sweet-spot' between high-profile attacks on large enterprises that can have payouts in millions of dollars but also bring along a lot of heat and scrutiny and attacks on individuals and solopreneurs with low payouts of a couple of hundreds or thousands of dollars. SMBs are unlikely to have sophisticated security countermeasures in place and even successful attacks are unlikely to attract law enforcement.

Healthcare organizations have always been a lucrative target for hackers due to the abundance of high-value health and personal data stored on their servers. Couple this with the high levels of service demands placed on the organizations, low levels of technical awareness and legacy infrastructure - and hackers can have a field day. Hackers have also focused on government departments at the local, state and federal levels due to the higher chance of payouts as extended downtimes at such organizations can cripple critical utilities, and political capital and jeopardize lives. The recent attack

on Colonial Pipeline compromised gas supplies across the entire East Coast.

The growing trend of using double or triple extortion tactics

Some ransomware gangs have now diversified into operating on a double-extortion model. This represents a major change in strategy with the extraction of data and data extortion in lieu of just encrypting data in situ. This means that criminals leverage not just one, but double or even triple avenues of threats to compel victims to make payments. The traditional strategy is that hackers encrypt company data and demand ransom in exchange for the decryption key. But in the newer strategy, hackers compel victims to pay by threatening to also disclose the breached data on the dark web. This comes into effect if the victim fails to make the payment before the deadline. This can be a terrible conundrum for organizations as this means their data could be freely accessed by any individual on the criminal-infested dark web network leaving them open to attack on multiple fronts from multiple sources. This potential for further exploitation often scares organizations into complying with the hacker's demands. Specific ransomware groups have also leveraged a triple extortion technique. In a recent example, a cosmetic company was hacked, and the perpetrators threatened to release the 'before and after pictures of their clients to the public. With access to **high-profile client data**, the hackers even contacted the clients themselves to extort them directly.

Leveraging advanced phishing tactics including spear phishing

Most readers are already aware of the kind of social engineering tactics that hackers leverage in order to carry out various types of phishing attacks. These attacks leverage different forms of communication such as emails, phone calls and texts that appear legitimate to the users and dupe them into taking actions as intended by the hacker. These steps can be anything from clicking on a link that delivers malware to their system or takes them to spoofed websites where their user credentials or banking details can be keylogged or posing as a trusted source such as a business leader or an agent from their bank asking users to carry out specific financial transactions and more. Spear phishing is a more advanced form of phishing that targets a specific target and is launched only after the hackers conduct extensive research on their intended victim. This research can be carried out through social scraping and other tactics. These attacks are nearly impossible to detect even for the most aware and security-conscious of users.

Proliferation of tactics used to target networks and backups

Hackers are no longer limiting themselves to encrypting targeted systems, but also damaging the networks. They are also launching high-impact DDOS attacks to flood and crash company servers, websites and leveraging other tactics to create an outage. Since many companies rely on **backups for data recovery**, backups have become a primary target for hackers. They tend to target backups first to delete or damage backups and sabotage the recovery process. They are also using advanced ransomware that is capable of lying dormant and undetected for months. This type of ransomware can lodge itself in legitimate files and delay encryption attacks for months before deploying. Meanwhile the ransomware builds a nest in the company's backup repositories creating an Attack-Loop™. This kind of attack tactic can result in the backups being infected or even turn the backup software against itself to modify retention timelines, authorized users and all other immutability restrictions. Hackers can also use sophisticated tools to find user credentials in the memory of compromised systems. They could also opt for a 'low-tech' approach wherein they harass end-users until they contact IT for support and collect the user credentials when the admin logs on to an end-user system.

Malware is getting harder to detect than ever. There is increasing evidence that hackers have now developed 'Anti-Anti-Virus Code' that is highly proficient in disabling all active anti-virus tools and Windows Defender. Hackers have even started to use embedded advertising in malware to try and recruit internal personnel as affiliates to carry out the attack. They are also embedding malware in PDF files and Excel Formulas (deeply embedded code in hidden excel sheets that can't be found through the GUI). Hackers also extensively leverage persistent malware that always stays active and copies itself into startup code of the system software. This means that the malware gets activated every time the user tries to restart or reboot the system and re-establishes remote access connections for the hackers. For attacks at scale, hackers leverage domain controllers, and even exploit windows group policy features to globally disable windows defender and seamlessly infect user systems across the entire network.

How can you protect yourself in the Ransomware 3.0 era?

While all of the endless techniques and strategies listed above can scare the wits off most users, there are many ways for enterprises to protect themselves better. The first step starts with understanding the gravity of the problem they face and taking security measures well in advance to mitigate attacks, if not prevent them entirely. Here are just a few methods:

Implement cyber security software tools that look for unusual behaviour

Basic ransomware attacks can be identified using anti-malware programs, but higher-order attacks such as zero-day attacks can only be prevented using advanced defensive technologies, such as:

- Endpoint detection and response
- Sandboxing
- Behavioral analysis
- Adopting a zero-trust approach to security and network access
- Deception technology

Network scanning to identify data exfiltration

Data exfiltration attacks can be hard to detect as they frequently mimic normal activity. Hackers often leverage network communications for data exfiltration. They use HTTP or FTP to transfer files and dupe incident response (IR) teams into thinking they are witnessing legitimate network traffic. Hackers can also leverage the TOR browser to hide all location and traffic data. This makes it harder for organizations to detect attacks before a portion of the data is already lost.

This is why organizations need a mechanism in place to reliably distinguish between unauthorized and authorized data transfers. A combination of defensive technologies such as data loss prevention (DLP), SIEM and UEBA offer the best solution. Security Information and Event Management (SIEM) enables organizations to conduct real-time monitoring and analysis of events. These tools are also capable of tracking and logging data for compliance or security audits. The benefit of using such technologies is that they can effectively uncover user behavior anomalies and leverage artificial intelligence to automate manual processes resulting in faster threat detection and incident response. SIEM solutions now also offer advanced user and entity behavior analytics (UEBA) enabled by AI and machine learning. This is an efficient data orchestration system that operates using artificial intelligence algorithms to determine baselines of normal and expected behavior and detect aberrations.

According to data from ESG research, 87 percent of companies use Network Traffic Analysis (NTA) tools for threat detection and response capabilities, and 43 percent consider it to be their first line of defense.

Training of all users in advanced cybercriminal tactics and cyber security best practices

Historical data often points to the fact that the greatest threat to organizations actually comes from its users. Humans are prone to errors, especially in high-stress situations. Social engineering tactics often leverage this to exploit users and compromise organizations. This is why continuous training in advanced cybercriminal tactics has to become a part of the security culture of any organization.

Employees must be continually aware of threats, know how to recognize and respond to them and implement all security best practices by default. Organizations need to focus on regular and consistent messaging on cyber security to all employees irrespective of rank or department. All users must be taught how to validate URLs, verify senders or avoid clicking on links or attachments altogether. Companies should also implement password managers to automate password renewal and enforce strong password creation policies.

Patch and update systems

A report from Osterman Research found that patching came a close second to multifactor authentication as the most effective tool against ransomware. Regular patching is critical for organizations as it can effectively shrink the attack surface (undefended areas) and reduce the chances of being attacked. Modern patch management tools are able to prioritize vulnerabilities and auto-assign tasks. Advanced vulnerability management tools are also capable of consulting threat feeds and schedule regular scanning of systems, applications and networks.

Protect backups from Attack-Loops™ and credential hunting

We have already talked about Attack-Loops and credential hunting. Now let's see what exactly happens during a ransomware attack.

- **Deleted backups** — If your backups are deleted, you lose access to all mission-critical data.
- **Failure to restore data** — Backup restoration processes fail.
- **Attack-loops™** — There's ransomware on your system and you try to restore from a backup. But every time you restore, the ransomware just gets activated again because it's lodged in your backups as well.
- **Long recovery times** — For most businesses, doing a clean restore and recovery takes an average of 22 days. All the while the business loses money.
- **High costs** — If you need to reconstruct systems and data from scratch (as was the case with Merck, a victim of the NotPetya ransomware), it could cost your business millions.

It's not an easy feat for any company to effectively navigate through the treacherous waters of a ransomware attack. This is where a comprehensive security solution such as Asigra Tigris™ can help. This is the most advanced backup solution currently in the market that can prevent ransomware attack loops from taking root in your backups. Tigris™ employs bi-directional malware scanning with AI and ML heuristic detection in order to effectively identify and block attacks at the pre-execution stage before each backup and restore cycle. It offers a range of cutting-edge defensive capabilities such as password-less authentication with deep MFA, soft deletes (even if hackers delete files, they remain recoverable) and AES 256-bit in-flight and at-rest data encryption. Tigris™ also makes use of variable repository naming and obfuscated backup files, so hackers can never aim at a static target when they are trying to erase backups. It also significantly simplifies the entire backup process with true agentless management. Companies deal with a low-code environment with less patching requirements and direct updates on end-point systems that improve security.

Tigris™ can be the right solution for companies that need a single scalable repository with central, multi-tenanted oversight. It enables companies to meet the most exacting RPO and RTO with granular recovery controls, 'self-healing' capabilities and restoration of corrupted files, easy restoration validation and more. Tigris™ also offers automated backup management and recovery that allows businesses to truly optimize their recovery processes.

About Asigra

Asigra provides a completely different approach to protecting data that is multilayered and features the industry's #1 ranked anti-ransomware software. We offer a suite of services designed to neutralize attack-loops, new dormant attacks, credential hunting, and much more. Through enterprise data protection and cloud SaaS protection, as well as compliance management, Asigra implements a seamless data protection process.

Next Steps

Talk to us about your backup software. If your backup software was engineered with Ransomware 3.0 line of design, it's time to re-evaluate your backup confidence.

Contact Us