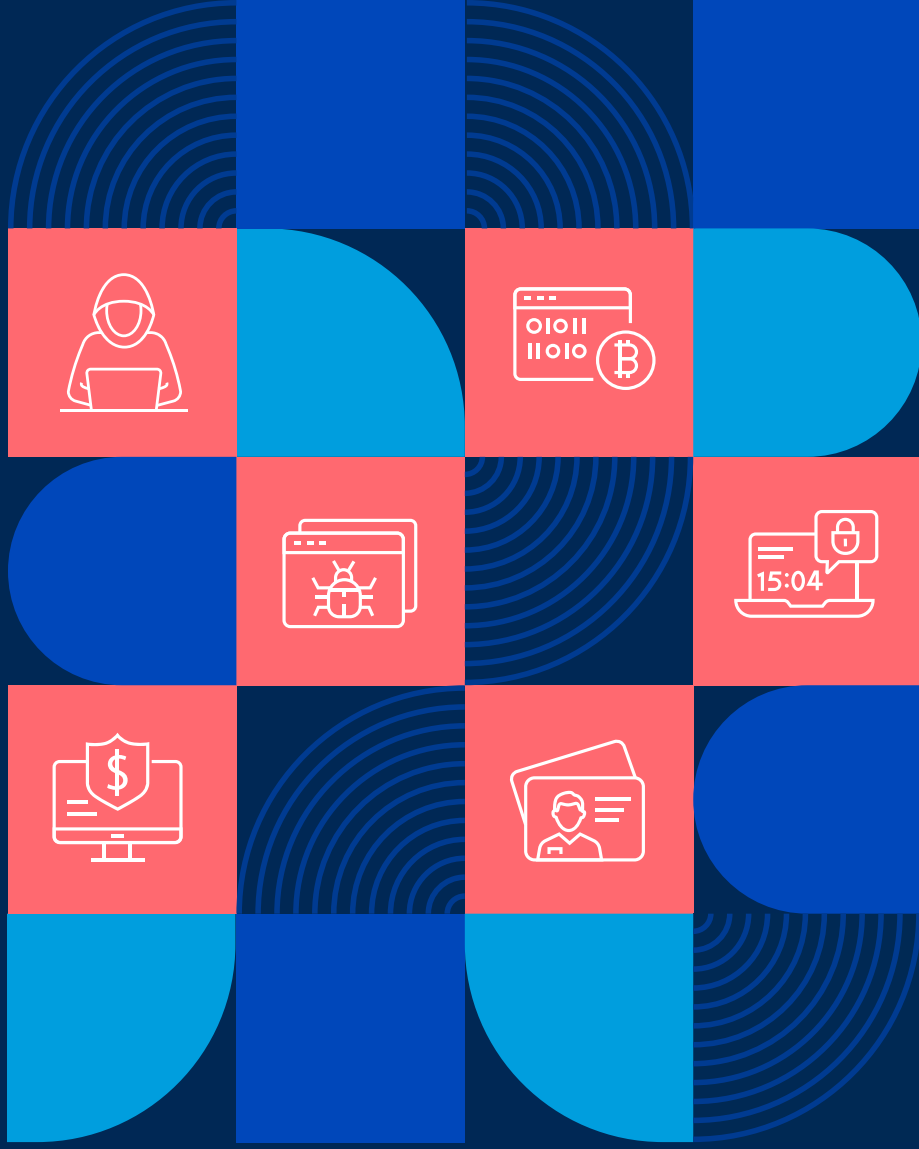
The Evolution of Ransomware – and How to Protect Yourself



Dropsuite

The Evolution of Ransomware Throughout the Years

The evolution of ransomware has seen a variety of malware forms emerge, leading to attacks that have maimed organizations and their IT systems throughout the years. The history of ransomware shows what was once a petty crime is now affecting major enterprises and economies all over the world.

Various types of ransomware – from the very famous crypto-malware to the highly-sophisticated big game hunting attack – are causing financial disaster for many companies, and MSPs are a key target. Ransomware attacks on MSPs have resulted in massive losses – and serious reputational damage – to the MSPs in question.

Organizations preparing for such attacks require proactive monitoring and defense systems and a secure backup and recovery solution: one that can heavily protect data and swiftly restore it in the case of a successful MSP ransomware attack.

A successful MSP ransomware attack is like a runaway train; once it starts, it can be near impossible to stop.

Ransomware was once considered a petty crime. Now, it is a major economic windfall for global criminal enterprises. However, this evolution of ransomware did not happen overnight.

The idea of how ransomware works – demanding ransom for user files and systems that are "taken hostage" – is quite old. The late 1980s witnessed encrypted files being held hostage by criminals in exchange for payment via the postal service. One of the first ransomware attacks ever was the AIDS trojan, a PC Cyborg Virus, released in 1989 through floppy disks. Victims had to pay $189 to a P.O. box in Panama to restore their access.

Ransomware stayed relatively stagnant due to payment collection difficulties until interest arose from the first modern variants introduced in 2005. These early ransomware attacks were mainly forms of "scareware," attempting to frighten users into buying phony antivirus software. They were usually unsophisticated, relying on panic more than advanced cryptography. Targets were usually able to reclaim their data easily.

Since then, ransomware attacks grew steadily but were still hindered by traditional and inefficient payment collection methods. Before cryptocurrencies, the only way to claim ransom was by using prepaid cash cards, retail shopping cards, and other jerry-rigged methods. Even with plenty of ransomware floating around online at the time, the difficulty of collecting on ransoms meant low damages overall.

When cryptocurrencies emerged – pioneered by Bitcoin in 2009 – everything changed. The growth of ransomware attacks truly began. Because this new mode of payment is easy to use and untraceable, criminals found it lucrative as a way to receive their victims' payments.

This set the scene perfectly for CryptoLocker in 2013. This new breed of ransomware harnessed not only the powers and capabilities of crypto transactions but also more advanced forms of encryption.

As ransomware evolved, attack efforts were optimized. Ransomware creators and operators decided to change tactics: instead of the "spray and pray" style of ransomware attacks that became common in the space, most began to focus on "big game hunting" (BGH).

BGH is a ransomware threat that utilizes the tactics, techniques, and procedures common in targeted attacks against larger organizations. However, instead of launching ransomware attacks against a huge number of small targets, BGH focuses the efforts on fewer but higher value victims that could potentially yield an even greater financial payoff.

THE EVOLUTION OF MODERN RANSOMEWARE

Big Game Hunting is a targeted, complex, low-volume, high-return cyber-attack executed using ransomware. As attackers gain entry to a network, they make lateral movements across the network to observe it, before exfiltrating files and deploying the ransomware.

The Various Types of Ransomware Attacks

Ransomware attacks restrict access to valuable files, data, and/or data assets and then demand payment for recovery. The evolution of ransomware has resulted in the emergence of various categories for this attack method. BGH is one; here are some of the others:

1. Crypto-malware

Key feature: Access to infected files is almost impossible without the attacker's decryption key.

This is currently one of the most popular and damaging types of ransomware; Typically, the user will discover that they cannot open files and will be confronted with a text document/popup with payment information. The entry point is generally malicious code embedded in a file of some kind.

2. Scareware

Key feature: After locking the infected unit, it displays a message claiming that an error or a virus has been detected, which is followed by a set of instructions on paying a certain amount to "fix" the problem.

This ransomware threat doesn't even need to "encrypt" files; rather, it can flood the screen with pop-ups and fake ads that prevent the user from utilizing the unit.

3. Lockers

Key feature: Locks the users out of the system entirely, preventing all access instead of merely encrypting select files.

Lockers also display messages in the infected unit, telling the user what the ransom demands are, often coupled with a countdown timer to induce panic upon the user and force them to pay the ransom without examining other solutions.

4. Doxware/Leakware

Key feature: Takes and encrypts personal and/or sensitive data, threatening to release it to the public or other parties if the victim doesn't pay up.

This attack targets highly sensitive data, and victims are often forced to pay the ransom for fear of being exposed. This type of extortion is now considered "big business" in the cybercrime space. News like this typically garners media attention, which threat actors often crave.

5. RaaS (Ransomware as a Service)

Key feature: This attack allows people who don't have the tools or the expertise to hire professional hackers to initiate attacks for them.

The person, referred to as an "affiliate", will split the ransom with the hacker as payment for their services. This also allows threat actors to focus more on developing their ransomware products since the affiliates find their targets for them.

Ransomware and MSPs

If an attacker gains access to databases that contain client credentials and other sensitive information, there's a high probability they'll gain access to thousands of business systems in an instant.

Cybercriminals will often look for any vulnerability that would enable them entry into a business' IT network. If they don't find direct access into an organization's systems, they will take the back door and attempt to enter through the enterprise's supply chain. Often, for businesses in the tech industry, managed services providers (MSPs) have the bad luck of being ransomware targets.

MSPs are essentially the "keepers of the keys" to their client's kingdoms, especially for their credentials. If an attacker gains access to databases that contain client credentials and other sensitive information, there's a high probability they'll gain access to thousands of other business systems instantly.

When ransomware attacks occur, not only are their clients put in danger; but MSPs suffer massive reputational damage. In an industry where security and trust are so important, such damage can mean they never fully recover (case in point: the Solarwinds incident).

To make matters worse, MSPs are under massive pressure to continue delivering their services 24/7 due to the COVID-19 pandemic, especially with more employees working from home.

The evolution of ransomware has seen it become the top mode of infiltration used against MSPs. A cyberattack through ransomware not only locks up data and prevents access, but can also spread into clients' systems once they succeed in infecting the main MSP network.

When ransomware attacks occur, not only are their clients put in danger; but MSPs suffer massive reputational damage, as well.

The Price Victims Pay

Ransomware damages are both reputational and financial. Many companies have lost millions of dollars to successful MSP ransomware attacks, on top of suffering brand damage. Here are some examples:

One MSP hit with ransomware was Cognizant. Hit by the Maze group in April 2020, the MSP estimated that it lost up to $70 million in various costs cleaning up the incident. While the attack did not affect any customers, many reported suspending their Cognizant services as a result.

Cybercriminals behind a cyber-attack on a Florida school district demanded a ransom payment of $40 million in cryptocurrency. The Broward County Public Schools' computer systems were compromised at the beginning of March by data-locking ransomware in a Conti gang operation. This attack caused a system shutdown but left classes undisturbed.

Computer giant Acer was hit by a REvil ransomware attack where the threat actors demanded the largest known ransom to date: $50 million.

These, along with the continuous increase in ransomware attacks, highlight the need for more security and preparation against such intrusions.

In a filing with the Securities and Exchange Commission (SEC), North American trucking and freight transportation logistics giant Forward Air Corporation said the December 2020 ransomware attack they experienced hugely impacted their fourth-quarter financial results. The incident was expected to result in the loss of an estimated $7.5 million of LTL revenue, mainly because it had to suspend "electronic data interfaces with its customers" the transportation company said.

The American MSP company CompuCom experienced losses of over $20 million following the DarkSide ransomware attack that took down most of its systems. ODP Corporation, CompuCom's parent company, revealed it "estimates the loss of revenue to be between $5 million and $8 million as a result of the incident (primarily because of CompuCom's need to temporarily suspend certain services to certain customers)."

The best way to guarantee data safety and security is with an automated, ongoing cloud-based backup solution that maintains complete copies of your emails, attachments, tasks and calendars, work documents, websites and databases in a separate, secure system.

Securing Workspaces Against Ransomware Attacks

Although proactive monitoring systems, firewalls, and related proactive protective systems can help reduce the risk of ransomware, they cannot guarantee data safety.Many companies have lost millions of dollars to successful MSP ransomware attacks, on top of suffering brand damage. Here are some examples:

The best way to guarantee data safety and security against the continuous evolution of ransomware attacks is with an automated, ongoing cloud-based backup solution that maintains complete copies of your emails, attachments, individual and shared drives, tasks, calendars, websites and databases in a separate, secure system. Should an MSP ransomware attack happen, you can restore your backed-up files easily and quickly — which can significantly reduce the impact such an attack would have.

Cloud-based backup and recovery solutions like Dropsuite reduce the impact of lost or corrupted data. Dropsuite protects a broad range of critical business data including:

- Microsoft 365 (email, SharePoint, OneDrive, Groups, Teams)
- Google Workspace (Gmail, Shared Drive, MyDrive)
- IMAP / POP Email

The benefits of Dropsuite's cloud-based backup and recovery solutions

1. **Automated Backup Process** - Users can back up Microsoft 365, Google Workspace or website files within 5 minutes and automate future backups. Incremental backups include unlimited storage and retention options to ensure you never run out of space.
2. **Easy Administration and Management** - Dropsuite's single-pane-of-glass admin panel with role-based access levels allows you to grant access easily to departments, groups and department admins. Companies can easily grant access to users outside their firm such as IT Admins, Compliance Reviewers, Other Users etc.
3. **Secure Storage** - Feel safe knowing that only you and those you designate have access to your backup emails and files. Your data is fully secured with TLS or SSL when available and is encrypted using military-grade 256-bit AES. Data is protected both in transit and at rest.
4. **1-Click Restore and Download** - One of Dropsuite's most popular features is 1- Click restore and download. Clients can easily restore or download single files, a set of files or all files to their computers. In case of accidental deletions (the most common form of data loss), clients can restore all using the 1-Click function.

The evolution of ransomware has produced various forms of attacks that put most companies at risk. The recent increase in ransomware attacks brought more danger as they started to infiltrate MSPs. A successful MSP ransomware attack is like a runaway train: once it starts, it can be difficult to stop.

MSPs can still ensure their data's safety beyond firewalls and other protective systems. Secure, cloud-based backup and recovery systems like Dropsuite reduce the impact of ransomware attacks on your systems and prevent brand and reputational damage.

To see Dropsuite in action, experience a live demo below.

Experience a Live Demo

"Just like everyone knows they have and will endure cyber-attacks and yet have no insurance, cloud issues and loss are bound to happen – and Dropsuite is the insurance they should have for that loss."

Matt Lee, Director of Technology and Security, Iconic IT