

Ransomware Is Growing More Pernicious; It's High Time Your Defenses Evolve

By: [Mark Greisiger](#) | June 3, 2020



Mark Greisiger has led NetDiligence®, a cyber risk assessment/data breach services company, since its inception in 2001. He has been responsible for the creation of solutions utilized by 100+ leading cyber risk insurers across the globe to support their loss-control and cyber education objectives. Mark can be reached at

Mark.Greisiger@NetDiligence.com.

Ransomware attacks and ransom payments for data continue to spike, with The New York Times reporting a 40% increase between 2018 and 2019.

As cyber threats go, ransomware is especially insidious, because these attacks, hitting everything from municipalities to banks to small businesses, often go unreported. That means less shared information and fewer actionable insights for insurers or insureds trying to arm against an ever-morphing enemy.

We saw a gap — leading incident response experts who work with the cyber insurance industry didn't have a forum to exchange information about what was happening on the front lines of these attacks.

We needed a way to get our arms around this problem to better support our cyber insurance carrier partners, a way to keep up-to-date and better understand the data trends from the expert's vantage point at ground level.

Enter the Cyber Insurance Ransomware Advisory Group, which NetDiligence assembled in early 2020. Featuring 20 members from leading breach incident response service providers — including Arete, Charles River Associates, CrowdStrike, Kroll, Kivu, Tracepoint, MOXFIVE, Tetra Defense and others.

The group meets quarterly and at select NetDiligence Cyber Risk Summit conferences to discuss emerging trends and best practices and make these insights available to the cyber insurance industry.

The Emergence of the Maze Variant

One of the key takeaways from the inaugural meeting was the emergence of the Maze variant and a “new normal” of data exfiltration, often including stolen private customer information.

Whereas previous generations of ransomware have been designed by threat actors to encrypt data and extort an organization for Bitcoin in exchange for the decryption key, Maze significantly increases the pressure on the victimized organization and threatens to make the stolen data public by releasing it on the internet.

This has magnified the potential loss exposure and has led to a host of new privacy data breach risks for insureds — with accompanying notification requirements.

Even clients capable of restoring files from secure backups may find themselves subject to privacy data breach impacts, such as the need to comply with state breach notification laws that include attorneys general and the victimized population, which significantly increases claim costs.

Ryuk Is Still Ever-Present

Another dangerous variant, Ryuk, continues to plague organizations with its tendency to attack both servers and workstations.

Experts expressed concern about organizations responding to Ryuk attacks with complete network shutdowns rather than impact isolation.

When assisting small- to medium-enterprises (SMEs), experts often find it challenging to convince management of the necessity of deploying automated malware eradication and remediation tools and to ultimately convince these organizations to keep endpoint protection in place once the immediate incident is resolved.

What Other Ransomware Concerns Are Out There?

Other specific ransomware types encountered include DoppelPaymer, Sodinokibi, Revel and Netwalker, as well as the continued rise of Ransomware as a Service (RaaS).

During the COVID-19 global pandemic, the impact of ransomware could prove devastating to an organization that may already be struggling.

Many of the widely-held notions about ransomware are changing, we found. After paying the ransom, some organizations may never receive the promised decryption key (in the past, certain threat actors were believed to be reliable).

Even with reliable threat actors, experienced negotiation can be critical.

Threat actors are also extorting organizations to pay for their encrypted administrator-level credentials. And, increasingly, ransomware impacts the backup files as well, encrypting or otherwise making them unusable for data recovery.

The experts reported that more than 50% of the time backups had already been exploited.

To Pay or Not to Pay

Nevertheless, recovering from a viable and segmented backup repository is still the preferred method of the majority of experts rather than paying the bad guys.

In fact, reported time for business interruption is much longer for cases where the ransom is paid — lasting from 3 to 15 days. If backup is used, business interruption typically spans 1 to 10 days, experts say.

This was a bit of a surprising finding: Members advised that the negotiation process itself, as well as problems encountered with the unreliable decryption keys, have contributed to delays with the Bitcoin payment path and extended the business interruption.

A Need for a Cyber-Ready Team

An ongoing concern for handling ransomware remediation is the difficulty for SMEs to respond in a timely manner towards the essential task of paying larger amounts of Bitcoin — or authorizing a third party to pay — for the ransom demand (averaging \$100,000, but based on severity ranging from \$400,000 to \$8 million, according to group members) within the given timeline for response.

SME clients often don't have the liquidity for these significant payments, even if their cyber insurer will reimburse them.

What's more, SME-sized IT departments are often unprepared to deal with this type of business interruption and may at times lack a functional understanding of cyber policy coverages and the supporting claims process, which forces them to learn on the fly during the moment of crisis in a ransomware event — underscoring that preparation is key.

Finally, the expert group reported that leading cyber security deficiencies that continue to haunt organizations include the usual suspects: lack of multifactor authentication, lack of next generation anti-malware endpoint protections, open remote desktop protocols, unsegmented backups and lack of employee training.

One thing is certain: The ransomware scourge is no fleeting trend. Experts believe that it's here to stay, inflicting damage as long as companies are willing to pay.

With the onset of COVID-19, ransomware attacks continue apace. While the nature of the attacks has altered slightly, their frequency has not, said Winston Krone, global managing director of Kivu Consulting.

Going forward, the Ransomware Advisory Group will continue to stay on top of these threats so that carriers and their policyholders can defend against them.

Quick Takeaways for Cyber Carriers and Covered Entities:

- Ensure that policyholders' management has in place an actionable data breach incident response plan that can be accessed at a moment's notice and includes vital third-party experts known to their cyber insurer.
- Offer a loss control checklist for SMEs of some baseline must-have cyber security measures to mitigate ransomware, such as multifactor authentication (especially in O365), endpoint protections (example CrowdStrike's Falcon Prevent), close remote desktop protocols, cloud-based backups and employee training. &

Reprinted from RISK & INSURANCE®, June, Copyright© 2020 All Rights Reserved.