ORION POLICY INSTITUTE

Why Ransomware is Rational and Why That is Good

Dr. Kall Loper
National Lead for Incident Response at Protiviti,
Professor of Computer Science at Southern Methodist University

Mike Lefebvre
National DFIR Lab Director at Protiviti

Orion Policy Institute

Orion Op-Eds
November 15, 2021

orionpolicy.org

Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no lon accessible because they have been encrypted. Maybe you are busy looking fo recover your files, but do not waste your time. Nobody can recover your file our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But y not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubl

Also, if you don't pay in 7 days, you won't be able to recover your files forever

We will have free events for users who are so poor that they couldn't pay in 6

How Do I Pay?

Dr. Kall Loper

National Lead for Incident Response at Protiviti, Professor of Computer Science at Southern Methodist University

Mike Lefebvre

National DFIR Lab Director at Protiviti

Ransomware attacks have made headlines for years, but understanding the true impact requires significant resources and access to the confidential, inner workings of their victims. In this work, we present a threat intelligence analysis informed by the resources and client experiences of a global cyber security consulting practice.

Ransomware attacks have evolved. Early forms were autonomous malware deployed to a victim network or system, typically through email or downloaded by the unwary. Later, victims were often targets of opportunity discovered through automated scans across the Internet seeking vulnerable servers. Now, they are part of an active intrusion and are only activated after stealing data.

Individual payouts can range in the tens of millions of dollars but insurance industry estimates place the average cost of an incident at around $250k for recovery and lost revenue. Tomorrow, ransomware attacks may be something new or they may go back to becoming another minor annoyance relegated to victims with low-security maturity.

The key factor in all these attacks is the denial, theft, or threat of exposure to monetize access to a victim's network. Briefly:

- Ransomware attacks deny the victim use of encrypted systems or data. This has a costly business impact and may force the victim to pay a ransom that is calibrated to be less than anticipated losses.

- Extortion attacks add to ransomware by stealing data and demanding payment to avoid public disclosure of the stolen data. Attackers have grown adept at selecting the scariest data to maximize their payout, including human resources, finance, business strategy, merger/acquisition, and sales/pricing data.

- Theft of data for immediate action has become a recent addition to extortion attacks. Attackers target data types sought in Dark Web marketplaces for auction. Short-lived data like valid credit cards is a low priority. Long-term data suitable for mortgage fraud, identity theft, and other credit theft is much more valuable. The trend of data theft corresponds with many threat groups breaking their informal ban on healthcare—a rich source of such long-term data.

At each step in its evolution, the ransomware attack has adapted to countermeasures such as the deployment of endpoint detection and response (EDR) tools or Business Continuity/Disaster Recovery (BC/DR) plans with sound data backups. Industry practices vary in effectiveness. The leading practice is to anticipate the attacker with cyber threat intelligence, adapt to the threat, and be ready to respond and recover if needed. Complex, layered defenses, and recovery capabilities are often deployed by the most valuable targets, such as those in the financial service industry. Industries with less regulation and a lower historic need for IT systems in operations tend to lag.

Ransomware attackers have innovated and specialized to manage evolving complexity of defenses. Threat groups broke up, differentiated services, formed cartels, or resurfaced under a new name. This activity and reorganization favored evolution as key players moved throughout the ransomware ecosystem taking their toolkits and expertise with them. Once, threat groups were synonymous with their tool. The tool was often named by the cyber security company analyzing victim's systems or honeypots owned by the security company. In a way, this helped ransomware threat actors brand their efforts and take a step toward the pseudo business organizations we see today. Today, ransomware groups or specific coders place their brand in the tool or offer the service under their brand on the Dark Web.

One of the more recent developments is a franchise model allowing affiliates to select victims and direct attacks using a Ransomware as a Service (RaaS) model. The threat groups defends their brand in an effort to build the victim's confidence that paying money will reverse the attack. Without some level of confidence, no one would pay the ransom. Economic relationships between elements in a stratified threat group bind threat actors to their established method of attack and slow revolutionary changes in favor of incremental changes. The innovation of stratified threat groups has become part of an understandable and therefore predictable ecosystem.

The key to understanding the actions of ransomware threat actors is to understand the economic rationality of their actions [1]. They seek to maximize profits from their investment of effort to build tools and compromise systems. Similarly, they seek to minimize the risk of exposure to law enforcement and nation-state retaliation. This is pure economic rationality, which is good for victims and potential victims seeking to secure their businesses.

There are indications that governments are starting to provide disincentives to paying a ransom. Payers risk prosecution under existing laws like those enabling the US Office of Foreign Assets Control (OFAC) sanctioned entity list. An additional risk is posed by payments to state-sponsored threat actors under the Foreign Corrupt Practices Act (FCPA) or through Anti Money Laundering Laws (AML) and regulations Such policies address ransomware victims through well-understood business risk and regulatory compliance.

----

[1] Politically motivated attacks by nation-state actors and their proxies have been the subject of speculation, but even with such attacks, the proxy group is often self-supporting or tolerated. A notable exception is the Notpetya attack on Ukraine in 2017. Numerous global-scope enterprises became collateral damage.

Non-governmental Organizations like the National Association of Corporate Directs (NACD) have joined regulators and insurance providers to influence corporate governance practices to include IT security. Boards of corporate directors ("the Board") see the increased need for Information Technology (IT)-focused members and even IT security-aware members. The Board is being prepared to engage with the business impact of ransomware. To counter such attacks, the enterprise can choose security investments or rationally accept risk. Corporate officers can present a rational story to deliver to the technologically aware Board. They anticipate the most likely threats in their environment. They prevent risk with prudent investments. They prepare to respond if the threat actualizes. They prepare to recover rapidly if needed. While not perfect, this compelling story of preparation is the best defense for corporate leaders in the event of an attack.

Ransomware is not good, but it is economically rational, and that fact is good for those of us seeking to counter it.

About the authors:

Dr. D. Kall Loper leads Protiviti's National Incident Response and Digital Forensics practices. He has 25 years of experience in DFIR and serves as a Professor of Computer Science at Southern Methodist University.

Mike Lefebvre is the National DFIR Lab Director at Protiviti and is a Computer Science PhD student with a dozen years of cyber field experience. Mike holds four information security-related patents along with his co-authors.

Photos by Unsplash

Orion Policy Institute is an independent non-profit think tank based in Washington D.C.

1050 Connecticut Ave NW Suite 500,
Washington, DC 20036
orionpolicy.org

Orion
Policy
Institute