Articles + Publications | June 23, 2021

Ransomware's Scary – Be Wary and Ready to Parry

Privacy & Cybersecurity Newsletter

WRITTEN BY

Theodore P. Augustinos | Molly McGinnis Stine

Ransomware is dominating headlines and creating unimaginable headaches. Ransomware has been deployed against every industry sector, and against municipalities and other government agencies. The resulting disruptions and consequences hit hard. Why is this threat growing, and what can be done to mitigate the risk?

What's New?

Recent interruptions to our energy supply and food chain have highlighted ransomware as the significant cybersecurity threat that it has been for the past several years. Hospitals, financial services companies, professional services firms, defense contractors and other manufacturers, energy companies, airlines and other transportation companies have all suffered attacks by threat actors seeking to extort ransom payments in exchange for the promise of decryption keys. As of April 2021, six industries sustained the largest number of ransomware attacks – health care, utilities, insurance/legal, software vendors, manufacturers, and ISP/MSPs.[1]

Ransomware has become more widespread with the proliferation of ransomware as a service, enabling ransomware developers to effectively franchise, or supply others as attackers. Ransomware attacks have also become more pernicious as actors routinely exfiltrate data before launching encryption malware and exert more pressure on victims to pay under threat of publication.

With this change in approach, the legal analysis of ransomware has changed as well. Victims may have argued in the past that the encryption of data on their own systems would not trigger applicable state breach notification requirements, which usually turn on unauthorized acquisition or misuse of certain data, often with a threshold that would not require reporting if the incident did not pose a reasonable likelihood of harm (in some states, limited to a risk of identity theft or fraud) to affected individuals. Given that exfiltration of data by attackers is increasingly common, however, the same breach notification requirements apply differently. It is more difficult to sustain a position that exfiltrated data was not "acquired," and that acquisition by a malicious actor (depending on the types of data) did not present a risk of harm. Therefore, more ransomware attacks result in notifications to affected individuals and state, and possibly other, agencies.

In the recent past, most ransomware attackers seemed to take a shotgun approach: find a way in, launch the attack, and figure it out from there. Today, however, ransomware attacks are often launched in connection with significant reconnaissance and intelligence gathering about the victim. Reconnaissance may include information gathering about the victim and its ability to pay, including the existence and limits of insurance coverage, and about the data, to focus in on more valuable data in order to justify higher demands.

Driven by these increased risks, the demand amounts and the amounts of actual payments have skyrocketed. According to a quarterly report from Coveware, a ransomware response firm,

The average demand for a digital extortion payment shot up in the first quarter of [2021] to $220,298, up 43% from the previous quarter.[2]

The blockchain analysis firm Chainalysis confirmed increased payouts:

Known payments to ransomware attackers rose 337% from 2019 to 2020, when they reached over $400 million worth of cryptocurrency. Attackers show no signs of slowing down in 2021, and have already taken in more than $81 million from victims so far this year. It's important to keep in mind that these are low-end estimates, and that the true numbers are almost certainly higher.[3]

These statistics also predate the headline-grabbing amounts reportedly paid by Colonial Pipeline, JBS, and others.

What Can Be Done?

Exercise an "ounce of prevention." Most ransomware attacks are introduced through phishing attacks. Awareness training pays dividends in this environment. Technical safeguards, such as multi-factor authentication to prevent continued remote access after credentials are compromised and (where feasible) restrictions on remote access from unnecessary locations, provide demonstrable value. Other points of entry are also available to attackers, so penetration testing, closing any open ports, and checking firewall settings also offer high return on investment.

But have the "pound of cure" ready. Knowing what data resides on what systems before an attack can save precious time and alleviate uncertainty. Once the data is encrypted, it may be difficult to prepare for and execute on notification plans if the nature of the data and the identity of affected individuals cannot be determined due to the encryption. Take all of the normally recommended incident preparedness steps, such as building your team; updating your incident response and disaster recovery plan to contemplate the peculiarities of a ransomware attack; reviewing your insurance policy; rechecking log settings and preservation; and revisiting the security and adequacy of your backups.

---

[1] https://blog.checkpoint.com/2021/05/12/the-new-ransomware-threat-triple-extortion/ (retrieved 6/13/21)
[2] https://www.cyberscoop.com/ransomware-extortion-demands-increasing-coveware/ (retrieved 6/13/21)
[3] Chainalysis, "Ransomware 2021 – Critical Mid-Year Update," May 2021 (downloaded 6/13/21 from https://go.chainalysis.com/rs/503-FAP-074/images/Ransomware-2021-update.pdf)

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber