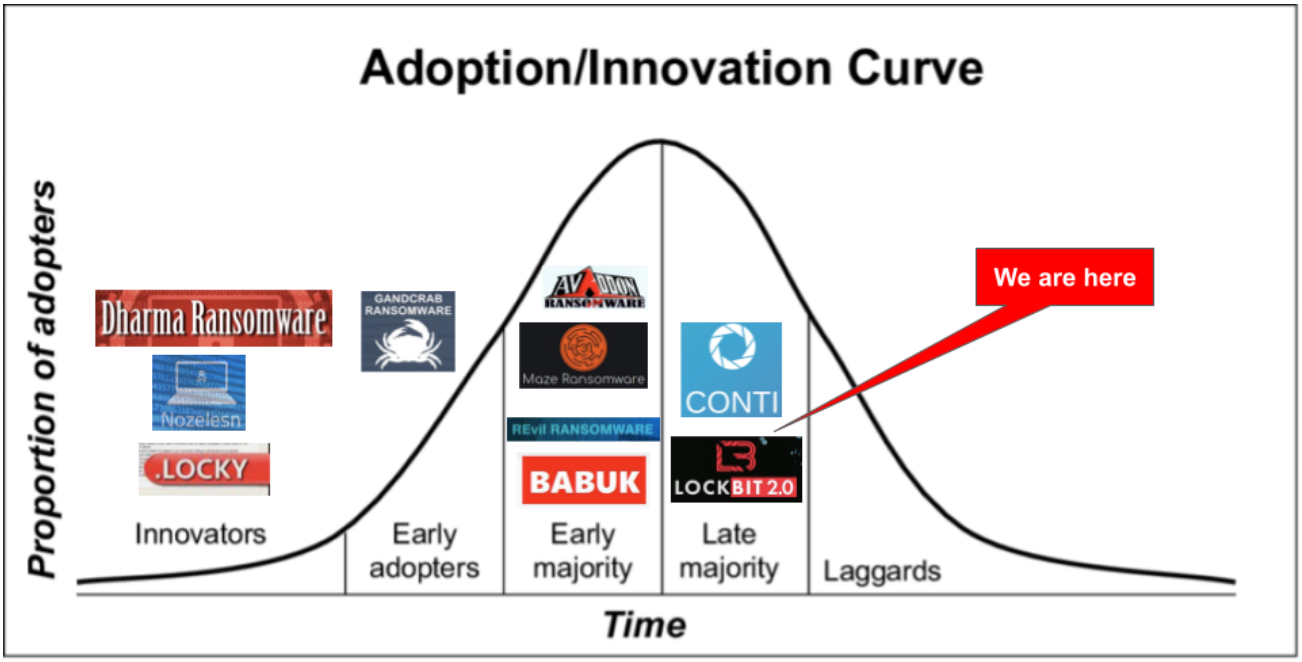
Ransomware as a Service Innovation Curve

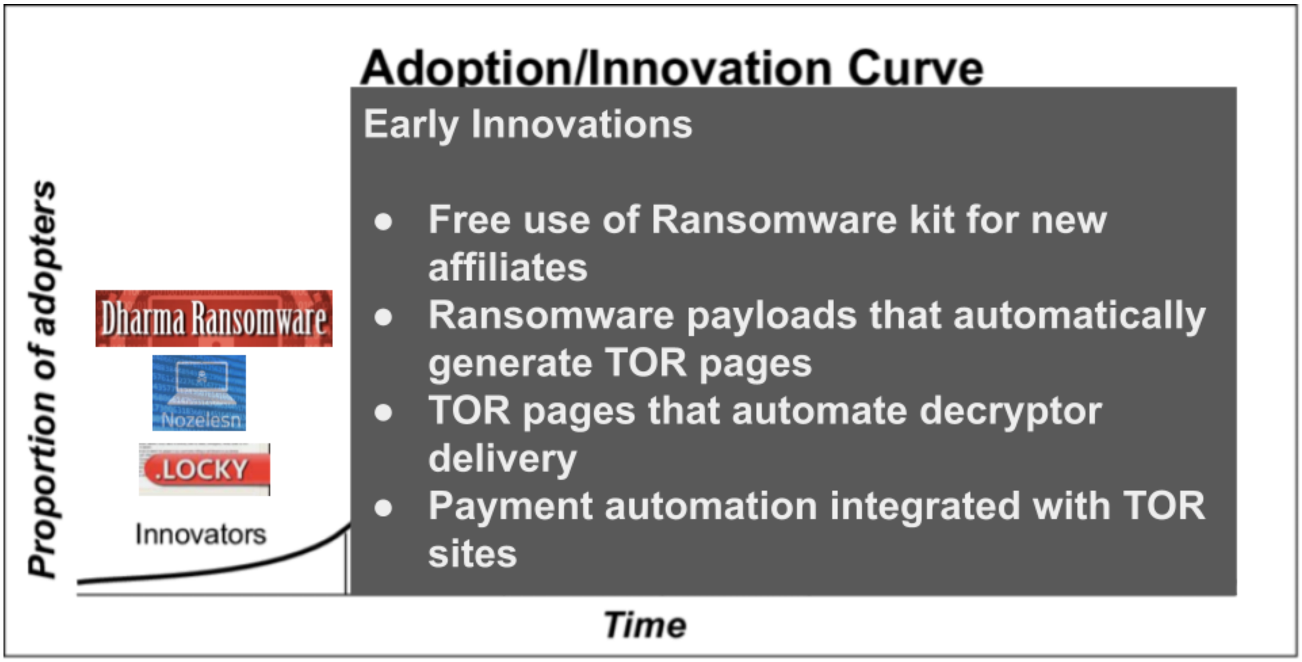
coveware.com/blog/2022/1/26/ransomware-as-a-service-innovation-curve

January 27, 2022

As we enter 2022, the evolution of Ransomware-as-a-service (RaaS) continues to be a driving force in the growth and permanence of financially motivated ransomware attacks. As we think about where the RaaS model may go in 2022, it is important to take a look backwards at the history of RaaS through a traditional economic / innovation framework. As we have often discussed, RaaS developers and affiliates have much more behavioral similarities to rational business operations than hardened criminals. Since RaaS operations traverse the same economic forces that legitimate business or industry would face as it matures, we can apply the Rogers Innovations Adoption Curve to think about where RaaS came from, and where it may go next.



RaaS Innovators (2016-2018)



Adoption/Innovation Curve

Early Innovations

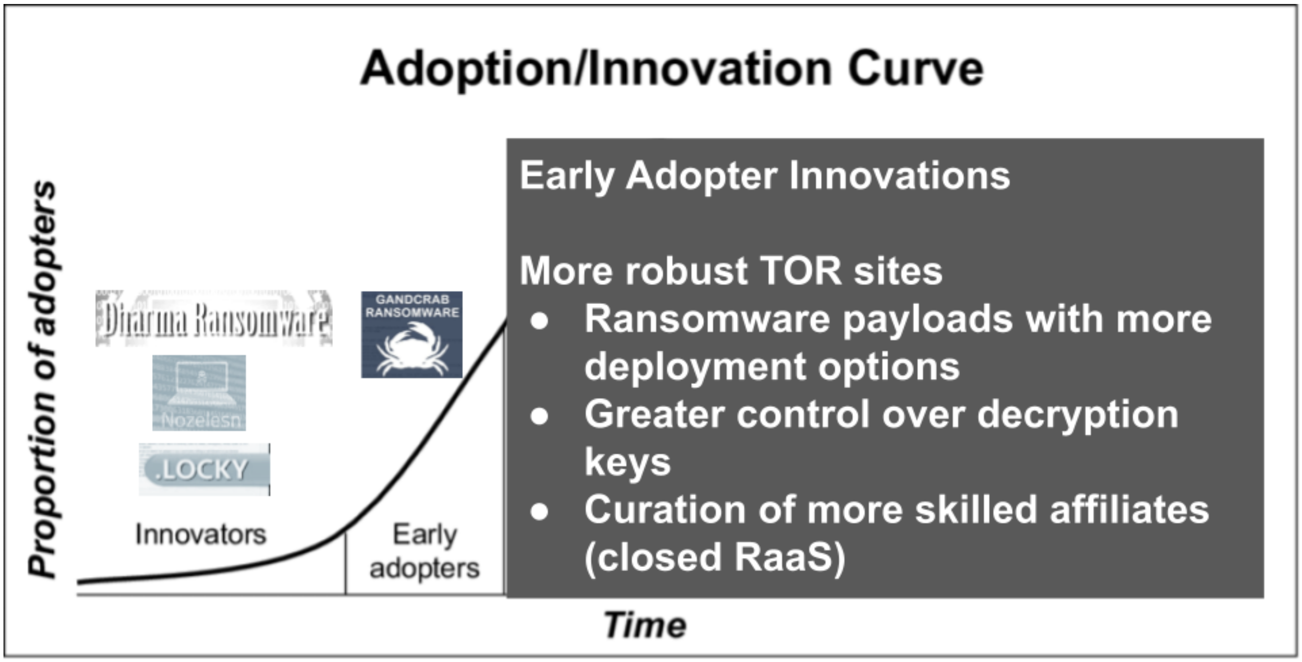
- Free use of Ransomware kit for new affiliates
- Ransomware payloads that automatically generate TOR pages
- TOR pages that automate decryptor delivery
- Payment automation integrated with TOR sites

Innovators to the RaaS model focused on lowering barriers to entry (attracting new affiliates to carry out lots of attacks), and creating efficiencies on monetization (i.e. getting paid more often and with less friction). The early RaaS developers would give their 'kit' away to new affiliates for free which greatly lowered the barriers to entry and made carrying out attacks more streamlined for affiliates. The other key innovation was TOR sites, like the one used by Locky ransomware. In 2016, this was one of the first RaaS operations to employ an auto generated ransom note that directed victims to a simple TOR webpage. The page had simple features, such as a test decryption portal and a "*pay $300 in BTC here*" button that provided a bitcoin wallet address. The page was also configured to release the decryptor once the ransom was paid to the correct wallet address. This automation allowed the RaaS developers to greatly scale their operations. Once they established an affiliate base of distributors, they could earn their proportion of ransom payments without needing to carry out attacks, or perform manual tasks.

This early version of RaaS was not without its issues though. One major complication was the affiliates' inability to assist with common decryption issues. Since affiliates only handled the attack and payment elements of the operation, they rarely had the technical know-how to assess why files weren't decrypting, or to determine what bug may be in the original malware that could be causing flaws in the encrypted file format. This also created a brand issue for the RaaS platform itself, as the ones with the poorest performances would eventually develop a bad reputation and lead a subset of victims to opt out of paying entirely.

Another issue was dishonesty among new recruits (i.e. the RaaS operator not having quality gates on who they allowed to use their ransomware kits). As the barrier to entry into the ransomware market evaporated thanks to the ease and availability of RaaS, so entered a new cohort of participants who did not care about the RaaS operations brand, let alone a victim’s unrecoverable files. As we will see, this issue would be addressed further along the curve.

RaaS Early Adopters (2018-2019)



Adoption/Innovation Curve

Early Adopter Innovations

More robust TOR sites

- Ransomware payloads with more deployment options
- Greater control over decryption keys
- Curation of more skilled affiliates (closed RaaS)

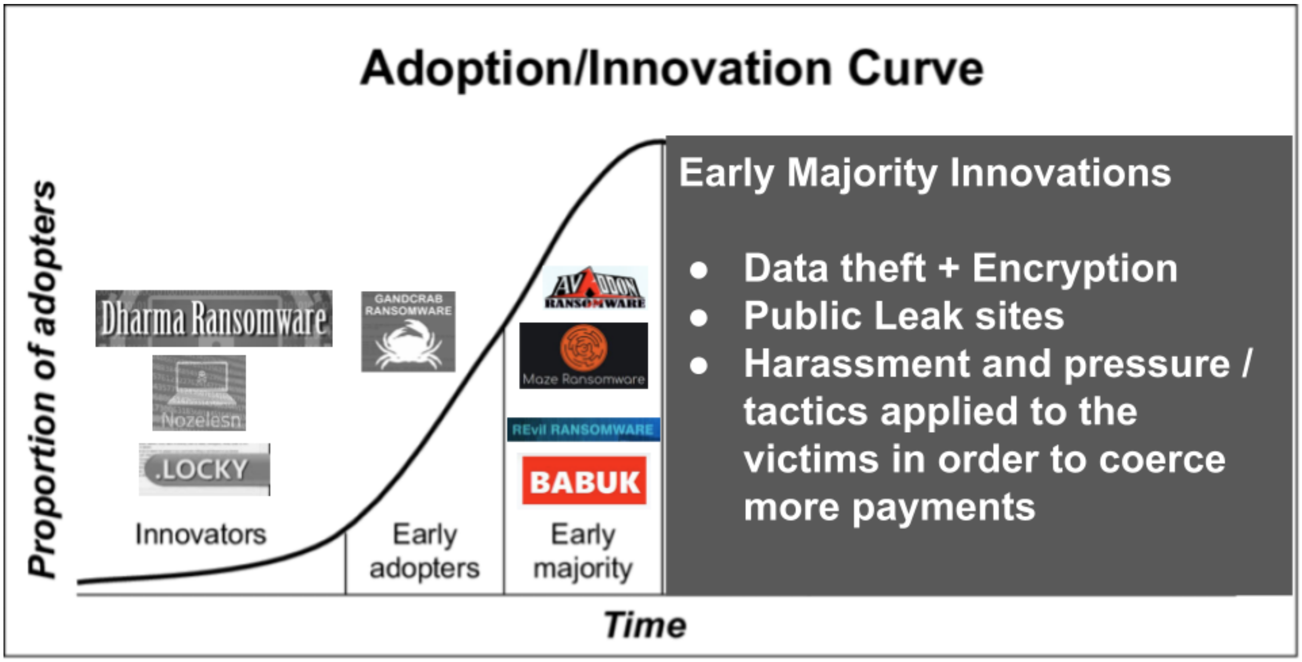
RaaS operators in the early adopter phase saw new applications and opportunities for innovation. The GandCrab RaaS platform was one of the key operations to explore how RaaS could begin to impact larger companies, and leverage new attack vectors (like MSPs) in their operations. The personality of the GandCrab group was also very similar to the traditional definition of NON-criminal technology Innovators. The traditional definition of early adopters reads as being *“eager to approach technological novelties but are more cautious of new trends due to their role as change leaders, which they do not want to lose. Early adopters are typically younger, have a higher social status, have more financial lucidity, advanced education, and are more socially forward than late adopters.”* This definition fits the personality of the original GandCrab operators that were much more brash with their ego, vocalism, use of forums and social media. Other innovations that GandCrab introduced:

- **Innovations in Extortion:** Centralization of negotiations at the developer level via TOR. This allowed many negotiations to be handled at the same time by the same operator. This also allowed the RaaS developers to enact quality standards to the negotiations and track their own best practices.

- **Innovations in Encryption:** GandCrab developed an encryption scheme that allowed each unique box to have its own encryption/decryption key. This enhanced their own security, but also allowed them to splice and split which machines a victim needed to decrypt. It also allowed for affiliates to innovate around more catastrophic distribution methods, such as attacking an MSP in order to encrypt all of the MSP's downstream clients. This innovation also had its drawbacks, and producing all the unique keys was very labor intensive for the RaaS developers. The GandCrab group would fix this issue when they moved to Sodinokibi ransomware and rebranded as REvil.

- **Innovations in 'Customer Service':** Unlike the pioneers of the RaaS model, GandCrab took a certain pride in making the decryption process as painless as possible for the victim. Not only did they remain on standby to provide detailed troubleshooting assistance (including new builds of the tool, if needed), their mission statement explained that in the unfortunate event a victim accidentally reinfected themselves within 30 days of the original attack, the decryptor would be provided to them again, no additional charge.

RaaS Early Majority (2019-2020)

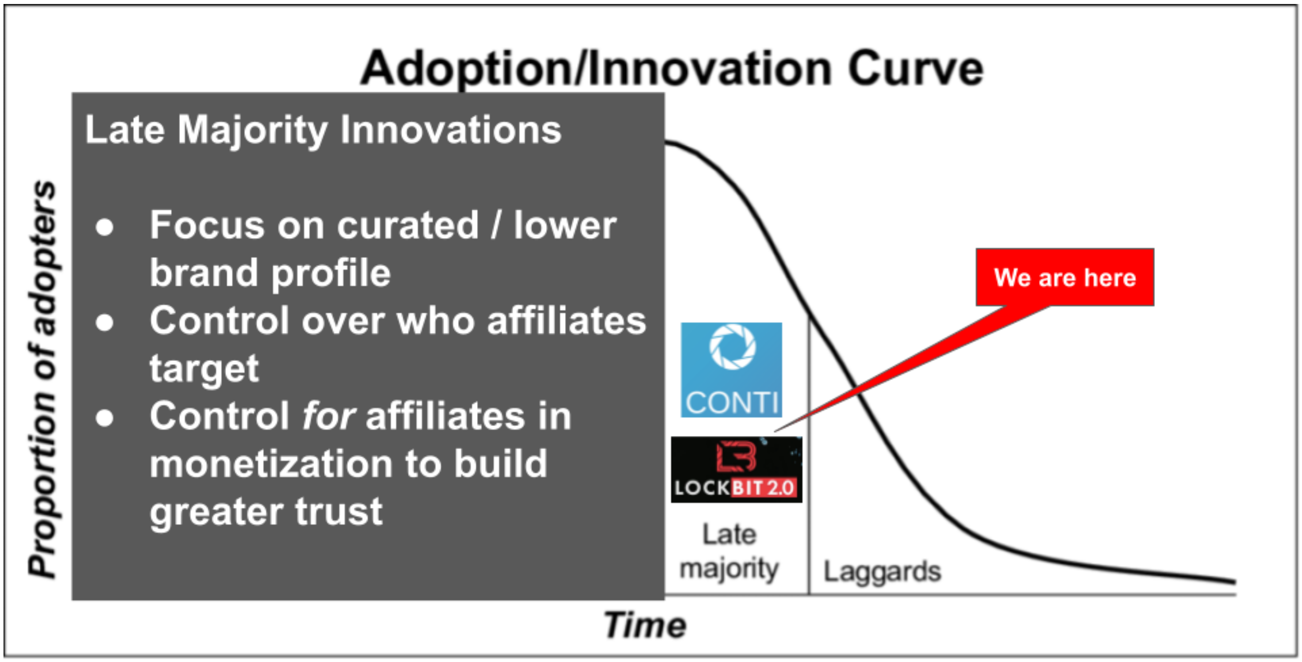


Early Majority Innovations

- Data theft + Encryption
- Public Leak sites
- Harassment and pressure / tactics applied to the victims in order to coerce more payments

Maze was the first major RaaS operation to demonstrate the efficiency and practical benefits of adding *data theft* as a requisite step in the extortion life cycle. Their tactics dismayed traditionalists as the stolen data had no actual value (i.e. it could not be monetized by other cyber criminals easily, like credit card numbers or stolen identities). Instead, Maze found value in the increased payment conversion rates they experienced on marginal attacks (that would have otherwise not paid any ransom but for the data theft aspect) when they mixed in the threat to damage the victim's reputation by leaking information stolen during the attack. Unfortunately, this trend received a groundswell of support from security media outlets that were eager to drive traffic by acting as distribution publicists for the RaaS operations. Bloggers and journalists began eagerly squatting on these leak sites, hoping to quickly amplify news of a new attack for their own benefit. This thrilled the community of RaaS operators, as now they had a publicity platform on which to back their threats. These Early majority RaaS operators also experimented with DDoS attacks against victims that were slow to negotiate. They would also enlist the help of outsourced call centers that would harass the employees or partners of victims that decided not to pay.

Late Majority RaaS 2020 - Present



Adoption/Innovation Curve

Late Majority Innovations

- Focus on curated / lower brand profile
- Control over who affiliates target
- Control *for* affiliates in monetization to build greater trust

Following the unprecedented actions of the Russian FSB to constript into service arrest a large number of REvil operators, the risk profile of being a RaaS operator has shifted. The main takeaway from these arrests may be to cut a lower profile (i.e. don't draw the IRE of the US government or other governments that may take disruptive or even kinetic actions against a group). The Conti group, while still quite brazen against US LEA, has tried to learn the lessons from DarkSide (who was responsible for the Colonial Pipeline attack) and has conspicuously avoided inflaming certain governments and industries (outside of their own) in their attacks. LockBit 2.0 has also tried to seize on some of the missteps of REvil.

Late majority RaaS operations are relinquishing control of the attack life cycle by allowing affiliates to handle the entire attack. They are also relinquishing more control over the outcome and, by extension, whether the attack actually results in revenue. It is up to the affiliate to ensure the attack is successful, that backups are compromised and that the encryption spreads far enough to inflict meaningful damage. If they fail, the victim is better positioned to restore from secure backups.

Further RaaS Innovation Trends to Watch

Ceding control to affiliates: Coveware's data shows that only **22.6% of victims in 2020 had viable backups**, but in 2021, this margin has jumped to **42% of victims.** This data point is surely influenced by multiple variables, but there has been a distinct drop in the number of cases where the threat actor was successful in rendering the backups useless. In parallel, we note that the percentage of cases involving the threat to release data continues to climb. We may deduce from these trends that threat actors are relying less on the operational disruption (harder from a technical perspective) of encrypted backups and more on the threat of sensitive data leakage to intimidate victims into paying.

RaaS operations like Conti and Lockbit 2.0 are ceding control over their 'brand' by allowing sloppy affiliates to carry out attacks without the victim's profile being vetted. While RaaS groups may SAY they don't attack hospitals or charities, most of them still do.The cybersecurity community is acutely aware of which extortion groups generally stick to their word, and which groups are routinely problematic and unreliable. In Coveware's YTD examination of 2021 attacks, **78.3% of re-extortion events were attributed to RaaS actors,** which is an increase from **66.7%** of re-extortion events in 2020. Re-extortion is a particularly nasty behavior wherein the bad actor signals to the victim that they agree to an offer, takes the money, and then informs the victim they need to pay another sum or they will get nothing. This behavior is observed far less when dealing with non-RaaS ransomware groups (such as closed RaaS or lone wolf groups).

Another equally damaging habit of RaaS affiliates is their propensity to **prematurely leak** victim information before negotiations have completed and sometimes before they've even had a chance to begin. **Over 90% of premature data leaks observed in 2021 were attributed to RaaS actors**.More concerning still is that of these disclosures where the actor responsible was part of a RaaS organization, **over 60% were from Closed RaaS** groups, which are historically more selective about who they allow in and - theoretically - should be more experienced and professional. We infer from this trend that either the vetting process for Closed RaaS recruiting has started to deteriorate and/or that contemporary ransomware actors do not place much value anymore on preserving their reputations as trustworthy hostage takers. Regardless, these increasingly volatile behavior patterns will have a direct and lasting impact on future victims' inclination to pay or not pay.

There have been other small innovations that RaaS operators are testing. Last month, security researchers reported that the FIN7 hack group was dipping their toes into the ransomware business not by advertising to new affiliates, but by trying to recruit legitimate IT practitioners under the guise of recruiting them to provide commonplace penetration testing services. As noted by Bleeping Computer, **“By creating fake cybersecurity firms to conduct attacks, Gemini believes it is an attempt to hire cheap labor rather than partnering with affiliates who demand a much larger 70-80% share of any paid ransoms.”**

Innovations in Affiliate Deception: Not all innovation is for the good of the community. In September 2021, Yelisey Boguslavskiy of Advanced Intelligence reported that REvil leadership had planted a backdoor into victim TOR negotiation chats that would allow them to discreetly scam their own affiliates out of a payment without the affiliate realizing anything was amiss. REvil affiliates were entitled to 70% of each ransom but with this magic trick, a REvil administrator could impersonate the victim and announce they were deciding not to pay, while simultaneously setting up a secret mirrored chat with the real victim to finish the transaction. News of this compelled the Lockbit 2.0 operations to advertise that THEIR affiliates could control 100% of the negotiation and payment, and only share proceeds on their own terms with the developers.

Balancing brand and LEA attention: The original draw of ransomware to cyber criminals was its inherent nature of being a low risk/high return enterprise. The explosion of ransomware attacks over the past several years has been fueled by innovation to the RaaS model. While the profitability has soared, the risk profile has substantially increased given the volume of LEA actions against RaaS groups and against infrastructure tools / tradecraft used by these groups. All high profile seizures and shutdowns of ransomware gangs in 2021 and 2022 were RaaS affiliate-based groups as opposed to non-affiliate based groups.