Ransomware Foundations Part One: The Multiple Layers of Ransomware Extortion and Beyond

Dane Grace

–

07.01.2022

www.halcyon.ai

halcyon

01 Modern Malicious Actors

The past decade marked a precipitous rise in ransomware as the attack of choice for cybercriminals. Malicious actors leverage encryption in their campaigns to render important files in accessible then demands a fee to regain access to affected data.

These attacks are so profitable that cybercriminals in 2022 mainly operate as meticulously organized services rather than lone wolf social deviants. Ransomware gangs often operated similarly to software as a service (SaaS) organizations in what is known as ransomware as a service (RaaS). RaaS groups separate the authors of the malicious payload from the operators of the associated infrastructure from the attackers who earn a portion of the ransom.

RaaS attacks have been described as human-operated ransomware in which teams of highly skilled hackers breach targeted endpoints and execute their campaigns in real-time. Once the victim's network perimeter is compromised, the team will adapt the attack route according to the circumstances of the compromised network and often leveraging existing tools in the environment – Powershell, Python and Group Policy Objects – to compromise additional targets.

This differs from traditional auto-spreading ransomware, which required the malicious payload to programatically propagate across the network. The challenge for the attackers in this scenario is that the scope of victim machines could be limited with network segmentation or, more drastically, taking affected machines offline. Cybercriminals now manually breach an environment before deploying a malicious payload, which ensures that they can affect as much critical infrastructure as possible.

Consider this example: A small health clinic with dozens of civilian patient records on its servers is compromised by a sophisticated human-operated ransomware attack. The patient records are now so thoroughly encrypted that the most powerful computer on earth today would take years to decrypt the data.

These records could contain individual drug sensitivities, vaccination statuses and other private details. A ruthless ransomware mastermind could quickly capitalize on these conditions and even cause a patient's death for the sake of profit.

Ransomware cybersecurity is still in its infancy, but defenses against these attacks have forced malicious actors to evolve their tools and techniques to apply pressure to targets.

The Rise Of Double Extortion Tactics

In many cases, denying victims access to their files will supply sufficient incentive to pay hackers the ransom. However, cybercriminals are implementing additional measures to profit from their cryptovirologic hosts.

Cautious organizations will back up their files and often do not trust hackers to lift the encryption once the ransom is paid. In these cases, hackers will encrypt, exfiltrate and threaten to leak the targeted data publicly if the ransom is not paid within a specified time window.

For example, consider a bank's private servers. A successful breach of this network could leave hundreds of customers' assets at the mercy of this cold-blooded hacker.

Encrypting, exfiltrating and threatening leaks has become known as "double extortion." The outcomes of this threat are undeniably devastating but do not represent the outer limits of the bad actors' tactics. There have been hundreds of documented cases where attackers will use triple and even quadruple extortion tactics.

Make That Double A Triple

Triple extortion will add a measure known as Distributed Denial of Service (DDoS). DDoS is not, in and of itself, a new cyberattack. The tactic involves the hacker purposely directing an enormous flow of internet traffic onto the target network's internet servers and overwhelming them until they crash completely after encrypting and exfiltrating data.

Here, the intent of this third measure to literally incite a "denial of service" to normal operations on the Internet. This means that legitimate traffic (i.e., the victim's clients, coworkers and contractors) are unable to perform daily business operations with the target firm. This disruption will halt almost all the victim organization's business operations online.

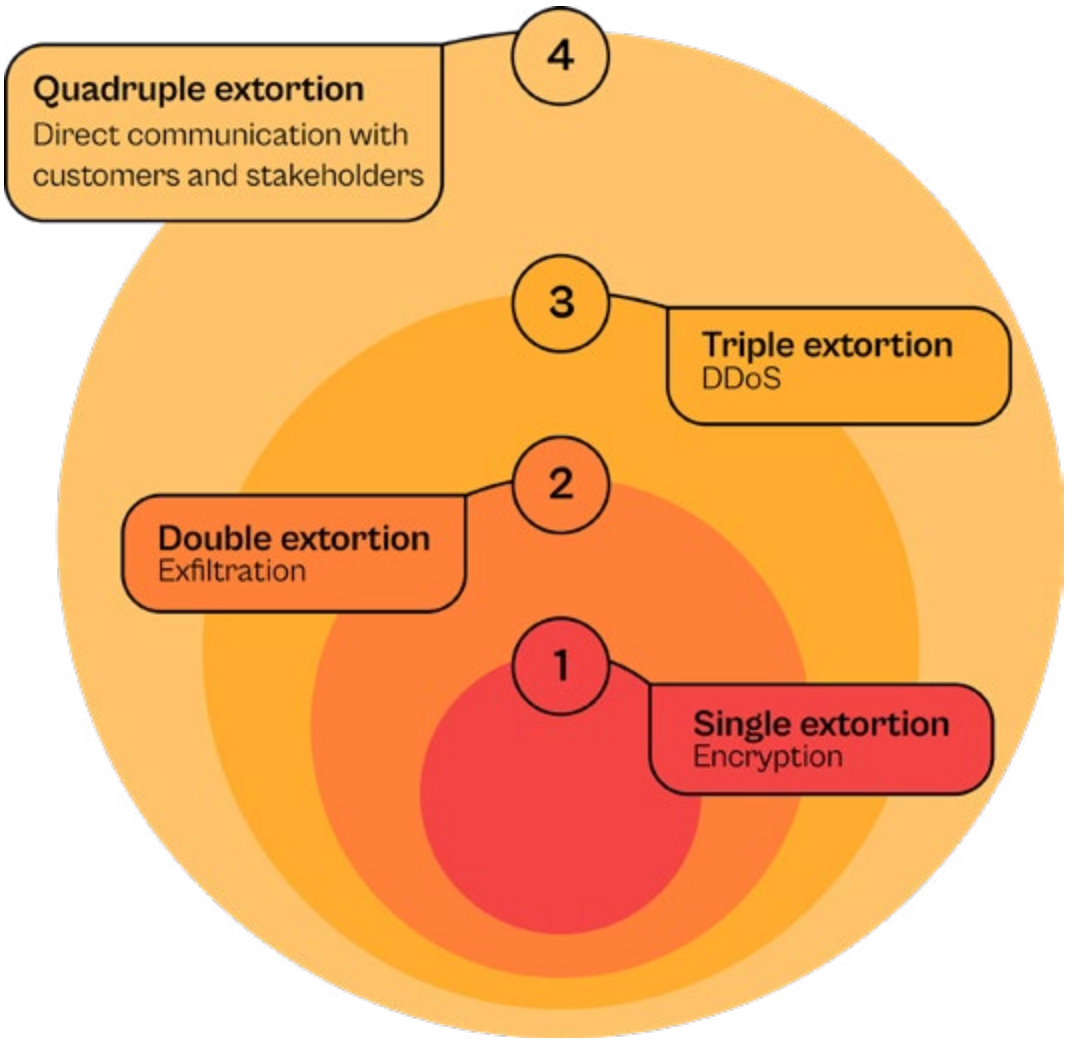
However, IT threat management teams have dealt with DDoS attacks for more than a decade and have devised mitigations to DDoS attacks. This is mostly positive news, but unfortunately, the hacking "industry" tends to attract some of the most resilient and tenacious workers in the IT world, who will almost always find a way to counter any cyber-defense measure.

This brings us to the appropriately named "quadruple extortion".

The Four-Pronged Attack

Quadruple extortion is a tactic employed by cybercriminals to further pressure victimized firms to pay a ransom. This method involves implementing the previous three measures and extending their influence by making threats to release confidential information on the public internet to an organization's business associates, customers or employees.

This represents a crescendo to a ransomware actor's timeline and is particularly damaging as it – by nature – involves damaging a firm's reputation or potentially spoiling vital business relationships.



The Future of Attacks

This multi-pronged approach to hacking organizations for monetary gain is only in its infancy. The scores of ransomware events in the past several years are a testament to the real danger these present to victim firms and the general population.

The most prominent example is the Colonial Pipeline breach in May 2021, which wreaked havoc in the Southeastern United Sates and caused fuel shortages and panic buying. Furthermore, the hackers forced the pipeline's senior leadership to pay a $5 million ransom.

Considering Prevention

This terrifying reality highlights the need for cybersecurity risk management and mitigation teams to start planning. What can we do to prevent such high-visibility ransomware attacks?

Security teams need to learn the tools, techniques and procedures of attackers, research defense strategies and implement defensive solutions to reduce or eliminate the threat of ransomware.

Ready to Chat? Contact Us

Halcyon is the industry's first dedicated, adaptive security platform that combines multiple proprietary advanced prevention engines along with AI models focused specifically on stopping ransomware. Halcyon is built by offensive security experts to stop attackers and was formed by a team of cyber industry veterans after battling the scourge of ransomware (and advanced threats) for years at some of the largest global security vendors. The Halcyon Platform is easy to deploy, does not conflict with existing endpoint security solutions and provides multiple, unique levels of protection against ransomware.

Want to learn more?

sales@halcyon.ai
+1.855.8HALCYON

halcyon