whitepaper

Ransomware Foundations Part Two: The Evolution of Ransomware

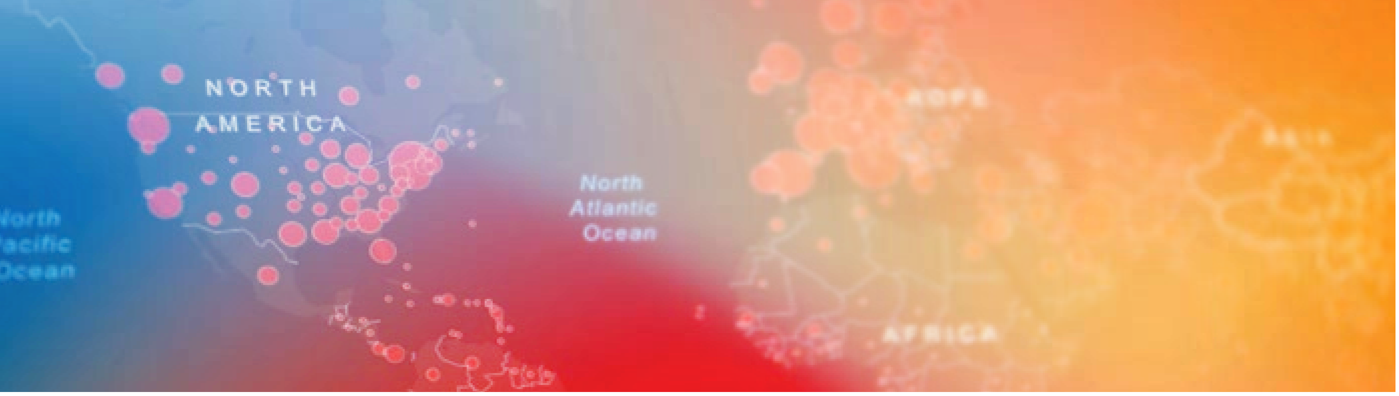
Dane Grace

–

07.15.2022

www.halcyon.ai

halcyon



02 The Evolution of Ransomware

Ransomware has made headlines over the past few years, and it seems that every week there is another news story about an organization victimized by ransomware. Security leaders need to understand what is driving these seemingly endless waves of attacks and the evolution from one-off breaches to criminal enterprises worth millions of dollars.

In the beginning, there was a floppy disk

The AIDS Trojan, named because the author was an AIDS researcher, emerged in 1989 and is widely accepted as the first case of ransomware. The malware was delivered via floppy disk to attendees of a World Health Organization conference. Once triggered (after multiple reboots), the malware encrypted files and demanded a $189 ransom to be sent via check to an address in Panama. The encryption used was easily defeated and investigators quickly identified the author as a certain Dr. Joseph Popp. Unfortunately, he was never tried after being declared psychologically unfit for legal proceedings.

Dissecting the first ransomware

The biggest issue with the original ransomware was that it was actually relatively trivial to recover from the infection. The author embedded the encryption method into the payload, which significantly eased reverse engineering and developing a method to recover affected files. In addition, shipping physical floppy disks to a specific set of individuals was costly, which limited the scope of the attack and provided reverse engineers with a static file source for analysis.

In addition, the payment method provided its own challenges for the fledgling cybercriminal and continues to be a challenge for ransomware gangs. Law enforcement relies on the tried-and-true tactic of following the money trail, and it is very straightforward to track down the perpetrator of the crime when that road ends at a checking account. In this case, the trail lead directly to Dr. Popp.

The payment problem

In the proceeding years, ransomware evolved to use more sophisticated encryption and attacks, but getting paid provided the greatest challenge, which reduced the profit motive.

Early ransomware actors demanded payment via credit card but finding a “friendly” payment processor to handle these payments was a challenge. Chronopay was one of the notorious providers and drove a similar increase in FakeAV scams. However, these fraudulent credit card payment processors eventually got shut down, and users also had the option to recover their money by resorting to the charge back service provided by credit card companies. At the time, this meant the revenues generated by ransomware were relatively modest and cybercriminals preferred other attack types.

Cryptocurrency becomes a factor

The appearance of cryptocurrencies like Bitcoin changed the landscape. Ransomware that demanded payments in digital currencies such as WinLock, Reveton and CryptoLocker appeared in the early 2010s and allowed for much larger ransoms. Simultaneously, or possibly as a result, the concept of Ransomware as a Service (RaaS) began to appear.

The RaaS model separates the actors into two groups: affiliates and the operators. Operators are primarily responsible for developing the malicious payload and operating the infrastructure needed to effectively run a ransomware campaign. The affiliates are primarily responsible for discovering targets, intelligence gathering and performing the breach that leads to extorting the victim. The Operator will then often handle processing payment and will pay the affiliate a portion of the ransom. This separation of concerns is primarily fueled by the switch to cryptocurrency as the primary form of payment.

In addition, moving away from simple encoded or embedded encryption algorithms to full RSA encryption and using a different key to encrypt and decrypt files, which rendered decryption without the key practically impossible.

WannaCry changes the game

Ransomware was already an established threat by 2017, but WannaCry and similar attacks like NotPetya arguably brought the threat to the cybercrime spotlight. Shadow Brokers - the WannaCry authors - leveraged a vulnerability dubbed EternalBlue that was discovered by and leaked from the United States National Security Agency to infect machines. Once the payload landed on a machine, it would scan the network for other machines with this vulnerability and attempt to infect those, which could result in exponential growth of the infection. Europol estimated that WannaCry alone affected 200,000 machines in 150 countries and could have been much worse had security researcher Marcus Hutchins failed to discover the kill switch that ultimately de-fanged the campaign.

This potent combination of ransomware and worm profoundly influenced how people think about ransomware and the first step in a response plan became disconnecting affected machines from the network "to stop the spread." While responders will frantically remove network cables from endpoints to limit the impact, the reality is that modern ransomware attacks are not using these "worm-like" capabilities to spread. Instead, attackers compromise large portions of the network in human operated attacks and the encryption is triggered at their discretion.

Attack vectors evolve

Email still accounts for a significant proportion of the initial entry point, but attackers are shifting to simpler and more focused attack vectors such as Remote Desktop Protocol (RDP) – which is a legitimate remote administration tool – to gain access. During the early days of COVID-19, many organizations were forced to quickly pivot their workforce from in-office to remote and unless configured correctly, RDP ports can be incredibly easy to discover and compromise.

In addition, there has also been a growth in "insider attacks," in which members of an organization are approached and offered compensation for installing a remote access tool or malware. This attack vector can be the most worrying because compromising a trusted relationship can render security tooling impotent.

Understanding ransomware gangs

Modern ransomware gangs are not a single entity. There is a full, thriving ecosystem of threat actors in play and a variety of tasks to complete, which include identifying victims, gaining initial access and supplying affiliates with intelligence.

Affiliates are the hackers that spend the time in the network, learn the infrastructure, identify the security tools in place and locating the victim's backup and recovery capabilities. The attackers will often leverage common tools already installed on the systems (called "living of the land" attacks) to move laterally, escalate privileges and ultimately steal valuable data.

Multi-factor (MFA) authentication has a critical role to play preventing lateral movement, but again, attackers adapt. Some attackers will simply flood the user with authentication attempts hoping that users will allow one, while others wait for the victim to authenticate and then piggyback on that session to gain access. However, some attackers will go to extreme lengths. They will impersonate a legitimate user and call the IT department to temporarily disable MFA because they have "lost their phone" or register a separate phone number so that they can authenticate via a device they control.

The actual ransomware encryption will be provided by the ransomware as a service "gang," but the deployment and triggering of the malware will usually be performed by a separate hacking team in a coordinated attack, with different parts of the network controlled by different members of the team.

It's worth noting that attacks are not restricted to Windows operating system. There has been a growth in using Linux-based tools and scripts as well. Ultimately, the operators will take advantage of whatever tools are needed. The attack is often triggered on the weekend or around national holidays to allow the encryption to complete while network defenders are less vigilant.

The ransom and the negotiation are usually managed by the RaaS team, and some even employ specialists to examine the data that has been stolen to determine the value. One of the most common questions is what happens if the ransom is paid? The short answer is that yes, a decryption tool will be provided. Some even have technical support to help their victims recover the data. It is, after all, a business. They must establish a reputation for providing the service they promise to remain profitable.

In Feb. 2022, an unknown actor leaked a trove of chat logs and other information from the Conti gang (it is speculated that the perpetrator was a disgruntled former affiliate), which provided a great deal of insight into how they run their business, the problems with recruiting, managing individuals and maintaining infrastructure. It became apparent that these groups suffer from the same challenges as many legitimate companies.

A word about Initial Access Brokers

Before an affiliate can begin an attack, they must first gain access to the victim's environment, and they often leverage Initial Access Brokers (IAB) as a shortcut.

IABs are criminal actors separate from the RaaS groups who leverage several techniques to gain access into target networks, which include malicious emails, impersonation over the telephone or scanning the public internet for vulnerable machines. Once they gain access, the cybercriminals will sell these stolen credentials to other groups, who are often ransomware affiliates.

IABs are an important member of the cybercriminal ecosystem and are often a cost of doing business for ransomware groups.

RaaS groups in the wild

RaaS operations have become the apex predator of the cybercriminal world – they are some of the most prolific malicious actors and generate more revenue than any other attacker type. However, their success belies vulnerability. The most obvious source of risk is law enforcement, but evolving defenses and internal betrayal are also sources of compromise.

» REVIL «

REvil, a prolific RaaS operator that was ostensibly shutdown but may have reemerged, provides a vivid illustration of perils faced by these cybercriminals. The group emerged in 2019 and claimed notable victims during their spate of attacks, which included a food processing plant and a contractor associated with United States Air Force, Army, Navy and NASA.

They seemed to operate with impunity until a multi-nation taskforce took down REvil's server infrastructure in October 2021. In November 2021, Operation GoldDust (a collaboration of 17 European nations) led to the arrest of five individuals associated with REvil. In the same month, the U.S. Department of Justice unsealed documents that revealed two additional suspects were arrested for their involvement with the ransomware group.

» CONTI «

Conti provides another example of the rise and fall of a seemingly unstoppable criminal force. The group emerged in 2020 and in the intervening years became one of the most destructive operators on the ransomware scene. Their playbook included affiliates gaining access to target networks via malicious e-mails, credentials acquired from IABs or fake software that was mistakenly installed. Once compromised, the affiliate would deploy the Conti ransomware and the operator would take over negotiating payment and delivering the decryptor.

Their rein culminated in a very high-profile attack on the national government of Costa Rica. The cybercriminals demanded a $10 million dollar ransom, which the government refused to pay. La Republica, a Costa Ricans business news outlet, estimated that the country lost $38 million per day in lost revenue tariff revenue due to the inability of customs officers to process imports via shipping ports.

A very public tit-for-tat ensued in which Costa Rican President Rodrigo Chaves declared a national state of emergency and publicly announcing that Costa Rica was at war with the ransomware group. Conti responded by calling on Costa Rican citizens to revolt.

Several weeks after the initial attack, the United States Federal Government posted rewards for the capture of significant Conti members. Ten days later, researchers discovered that important pieces of Conti infrastructure went offline, which ostensibly meant that the group disbanded. The reality is that Conti most likely shuttered because the “brand” became so toxic that the team feared capture and/or refusal to pay from future victims.

» LOCKBIT «

LockBit has become one of the most prominent RaaS actors in the wake of Conti’s apparent dissolution. The malicious payload utilized by affiliates is under active development and the most recent version migrated from the Go programming language to Rust, which provides several advantages including increased performance. Affiliates have reportedly victimized more than 200 organizations and even managed to outperform Conti in 2021.

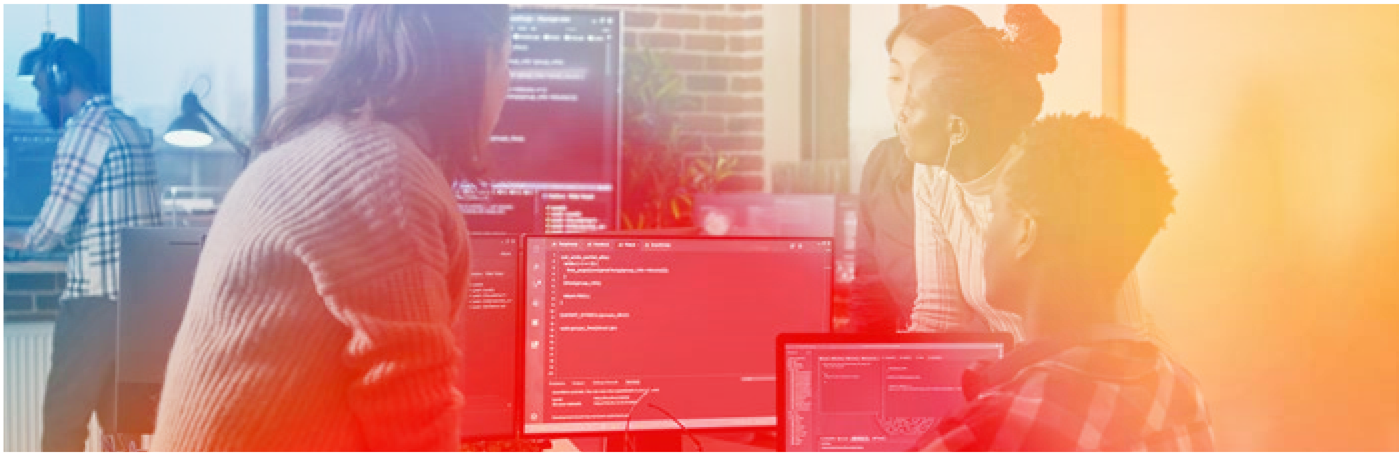
This group is currently active, but time will tell if they will fall into the familiar cycle of emergence, success and disbandment.

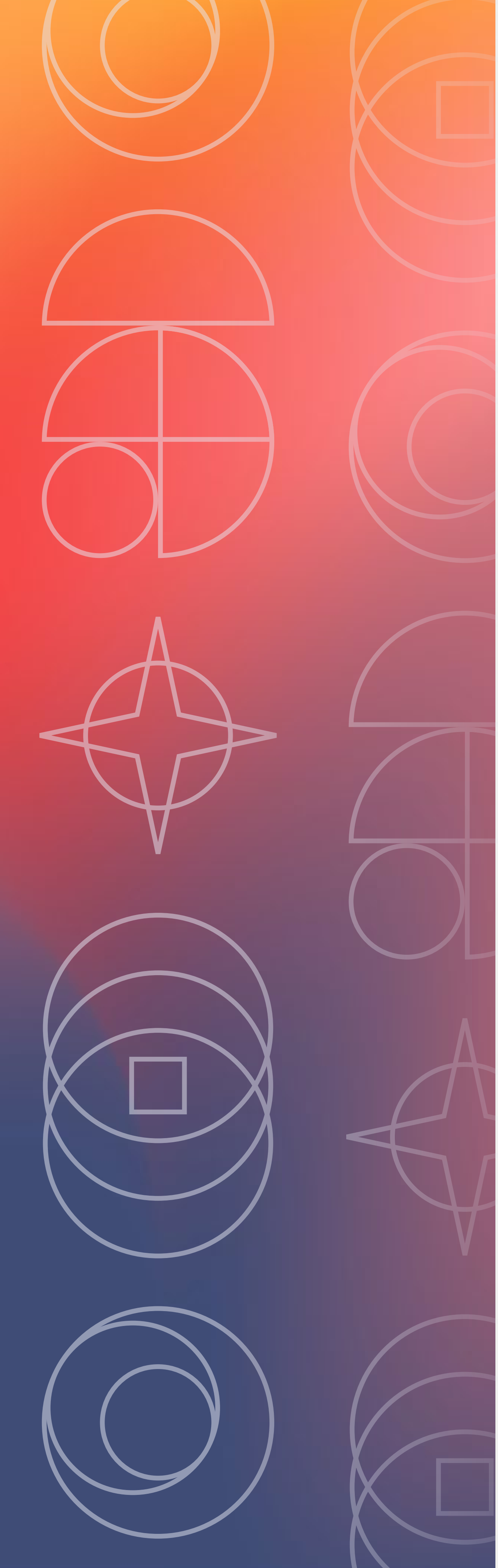
Conclusion

Ransomware is not a new phenomenon, but it has developed into a large-scale, wildly popular business that evolves and adapts according to circumstances. It is no longer a “spray and pray” type of malware attack. Instead, attackers use all the tactics and techniques at their disposal to target specific victims.

A strong defense begins with an assumption of vulnerability and prioritizing multiple measures to address risk. The aim is to reduce attackers the probability of success by deploying security tools and establishing robust processes and procedures. In the event of an infection, responders must have visibility into endpoints and the ability to detect malicious behavior as early as possible.

Finally, and as a last resort, recovery measures should be well-defined and understood by everyone involved in the defense of an organization. This includes minimizing downtime and restoring data to a usable state in order to reduce reputation damage.





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