

The Evolution of PINCHY SPIDER from GandCrab to REvil

crowdstrike.com/blog/the-evolution-of-revil-ransomware-and-pinchy-spider/

Adam Meyers

July 6, 2021



For years, ransomware was a nuisance that impacted individuals who were unfortunate enough to encounter it via banking trojans, exploit kits or phishing attacks and resulted in a large number of small-value ransoms — typically hundreds of dollars per incident.

In 2016, a terrifying new model began to emerge fueled by reports of high-value ransom demands targeting hospitals and medical facilities that were forced to pay ransoms in the tens of thousands of dollars (see: “Ransomware: Understanding the Threat and Exploring Solutions,” Statement from Adam Meyers for the Senate Judiciary Committee’s Subcommittee on Crime and Terrorism, May 18, 2016). These attacks, which we now call “big game hunting” (BGH), were conducted by well-known criminal groups using existing banking trojans that were repurposed for enterprise ransomware attacks. This model of attacking the enterprise illustrates that attackers realized they could make far more money going after highly targeted organizations. These targets started with healthcare but quickly morphed to large organizations that could calculate downtime in lost revenue, where at some point not long after the attack, the cost of being offline was higher than the ransom demand. This is what the attackers were counting on, and as such we observed manufacturing,

technology, industrial targets, state and local governments, and school districts all becoming attractive targets for big game hunters — organizations and verticals that often lagged broader industry in terms of security sophistication.

The Advent of RaaS (and Emergence of PINCHY SPIDER)

What began with closed specialized groups conducting these attacks soon morphed into ransomware as a service (RaaS), where a small circle of developers with criminal intent would create a platform for building encrypters and decryptors, and managing the ransom notes and payment portals. These groups would take on affiliates, known in Russian slang as “partnerkas,” who would leverage the platform for the actual ransom activity and be responsible for the targeting, deployment and execution of the attack. These affiliates would then share the revenue with the platform operators for the privilege to use the service.

In early 2018, one such RaaS, named GandCrab by its developers, hit the underground markets. The early versions of GandCrab had some implementation flaws, and the developers learned lessons that helped refine their business model. For example, early versions of GandCrab exchanged cryptographic keys insecurely, and organizations that recorded all network sessions could recover the keys. GandCrab operators initially sought partners to help them evolve the platform by offering a revenue-sharing model, which continued to evolve over the years.

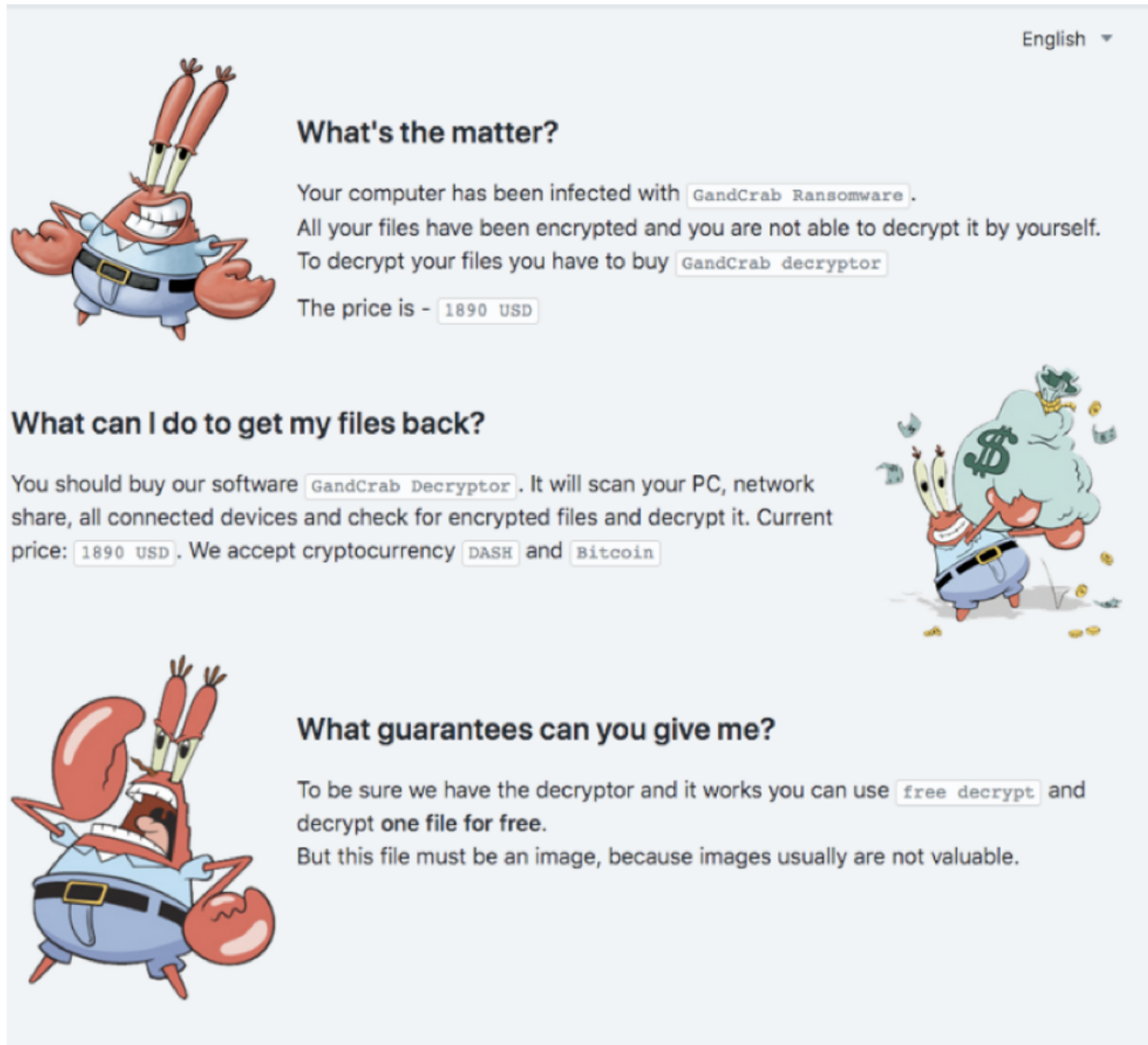
Some of the prohibitions for the affiliates of GandCrab included:

- Targeting machines in Russia and other Commonwealth of Independent States (CIS) countries (the malware will not infect machines using these keyboards and other parameters specific to these countries)
- Using unverified antivirus scanners
- Publicly listing the admin panel `.onion` address
- Reselling accounts

One of the notable differentiators for GandCrab included payment via the Dash cryptocurrency. Shortly after the introduction of GandCrab, the payment portal was compromised, resulting in free decryptors being published. The adversary (i.e., GandCrab developer) responded by announcing a version 2.0 would be available as a result, which they made good on within a week.

CrowdStrike began tracking this ransomware platform developer as PINCHY SPIDER, observing that they continued to innovate with newer versions of the ransomware. Version 4.2.1 for example was released as a result of an antivirus company releasing a “vaccine” for version 4.1.2, indicating that PINCHY SPIDER actors were continuously monitoring social media and open sources for discussion of their tools. As the end-of-year holidays rolled around in 2018, PINCHY SPIDER announced that they would have limited support during the holidays but would release a new version by the Russian Orthodox Christmas. GandCrab

operations continued to improve and develop throughout the first half of 2019, but on May 31, 2019, they announced, “All good things come to an end,” claiming their affiliates made \$2 billion USD over the previous year and that PINCHY SPIDER themselves made \$150 million USD. They announced that they would be shutting down in 20 days and that victims should pay or lose their data forever.



The screenshot shows the GandCrab ransomware payment portal interface. It features a cartoon crab character with a blue shirt and black belt. The interface is in English, as indicated by a dropdown menu in the top right corner. The main text reads: "What's the matter? Your computer has been infected with GandCrab Ransomware. All your files have been encrypted and you are not able to decrypt it by yourself. To decrypt your files you have to buy GandCrab decryptor. The price is - 1890 USD". Below this, there is a section titled "What can I do to get my files back?" which states: "You should buy our software GandCrab Decryptor. It will scan your PC, network share, all connected devices and check for encrypted files and decrypt it. Current price: 1890 USD. We accept cryptocurrency DASH and Bitcoin". To the right of this text is an illustration of the crab character carrying a large green sack with a dollar sign on it, surrounded by falling money. At the bottom, there is another section titled "What guarantees can you give me?" which says: "To be sure we have the decryptor and it works you can use free decrypt and decrypt one file for free. But this file must be an image, because images usually are not valuable." To the left of this text is an illustration of the crab character with its mouth wide open, showing its teeth.

GandCrab Evolves Into REvil

As the GandCrab samples stopped being identified and the payment portal was decommissioned, another ransomware began to become more prevalent, first identified a few months earlier and known as “Sodinokibi.” This new ransomware shared technical overlaps as well as distribution and operational overlaps with GandCrab, leading

CrowdStrike Intelligence to suspect these two ransomware were related. By July 2019, “REvil” became another name for this new ransomware, which quickly became one of the more prevalent ransomware tools observed.

By December of 2019, a managed service provider (MSP) became a victim of PINCHY SPIDER’s REvil ransomware, demanding a \$6 million USD payment. At the time, CrowdStrike Intelligence noted they “will likely continue to compromise managed service providers and make use of remote management software to spread REvil ransomware in order to ransom many companies from a single point of entry.”

As the world became impacted by the COVID-19 pandemic in early 2020, PINCHY SPIDER started capitalizing on a new trend of stealing data and further extorting the victim to pay for their data to not get publicly leaked, suggesting that victims might be subject to fines due to the EU’s General Data Protection Regulation (GDPR) if they did not pay.

In May 2021, the Colonial Pipeline ransomware attack made headlines across the globe, prompting the U.S. government to make statements about the attack and its implications. This attack was associated with another RaaS known as DarkSide, which CrowdStrike associates with CARBON SPIDER. As a result of the increased attention, PINCHY SPIDER issued new rules for their *REvil* RaaS affiliates, including the need to screen potential ransomware victims prior to infection. Only a few weeks later, PINCHY SPIDER was associated with a second breach targeting JBS, which resulted in additional statements from the U.S. Department of Justice indicating that ransomware investigations would be conducted similar to counterterrorism investigations. This prompted someone associated with PINCHY SPIDER to state that they were lifting targeting prohibitions, stating: *“It no longer makes sense to avoid working in the United States, all restrictions have been removed. You can work in all types of activities of a given state.”*

Protection Against PINCHY SPIDER and REvil

PINCHY SPIDER remains one of the most prevalent threat actors in the ransomware and data extortion space. Protecting against this type of threat requires organizations to get serious about security. Hope is not a strategy, and organizations closing their eyes and hoping they aren’t going to be hit by ransomware will not work. Here are five things that can help:

Secure the enterprise: This is what security experts have been saying for two decades: Ensure that the enterprise is defendable. Implementing sound security methodologies, patch management, vulnerability tracking and Zero Trust go a long way to help drive security and make an enterprise a harder target. (See the recent U.S. cybersecurity Executive Order and our blog post, “New Cybersecurity Executive Order: What It Means for the Public Sector.”)

Engage the threat: Waiting for the attacker to come to you is a dangerous precedent. Threat hunting ensures that any security incident, no matter how small, is investigated by dedicated hunters who go out and look for trouble. If you can engage these threats quickly before they elevate privilege or move laterally, you can prevent the ultimate objective, whether that is information theft or ransomware.

Next-gen tech: Signature-based antivirus technology doesn't cut it anymore. Machine learning classifiers that can determine if something is malicious based on its behavior or other observable traits are table stakes for defending the enterprise today.

Tabletop exercises: You play like you practice. You can have the best backup solution in the world, but if you have no idea who to call, which systems to bring up first, or have never tested the recovery at scale, then you're doing it for the first time during a major incident. A tabletop exercise can help build the muscle memory that an organization needs so that its teams know what to do when a situation presents itself. These can be conducted quarterly or even monthly and have different scenarios to help ensure that everyone is training for different threats.

Intelligence: There are dozens of different big game hunting adversaries that operate today. Understanding how they operate, who they are and what they target can ensure that your enterprise defenders are ready for the threat and know what to look for.

Additional Resources

- *Learn more about PINCHY SPIDER, CARBON SPIDER and other ransomware adversaries in the [CrowdStrike Adversary Universe](#).*
- *Download the [CrowdStrike 2021 Global Threat Report](#) for more information about adversaries tracked by CrowdStrike Intelligence in 2020.*
- *See how the powerful, cloud-native [CrowdStrike Falcon® platform](#) protects customers from DarkSide ransomware in this blog: [DarkSide Goes Dark: How CrowdStrike Falcon Customers Were Protected](#).*
- *Get a full-featured free trial of [CrowdStrike Falcon Prevent™](#) and learn how true next-gen AV performs against today's most sophisticated threats.*