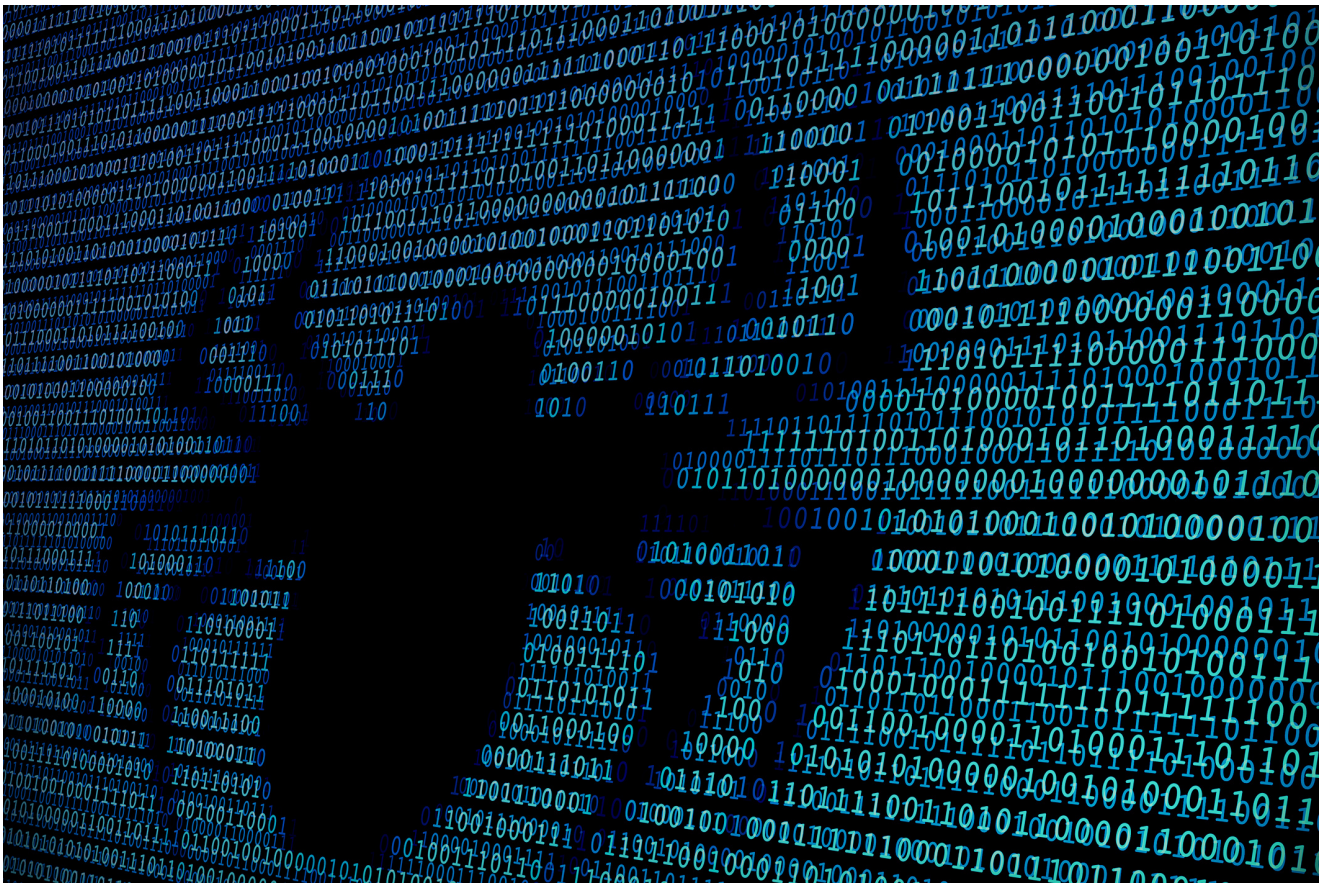
Ransom Mafia - Analysis of the World's First Ransomware Cartel

analyst1.com/blog/ransom-mafia-analysis-of-the-worlds-first-ransomware-cartel

Jon DiMaggio



Analyst1 spent time digging through criminal marketplaces where Cartel gangs have a presence to research and analyze the criminal entities within the alleged Cartel. We explored the malware and tools the groups use, tracked their bitcoin transactions, and studied relevant reports from other researchers in the field alongside select media outlets. Our research identified several key findings which are further detailed in our white paper "Ransom Mafia: Analysis of the World's First Ransom Cartel" such as:

1. Analyst1 observed Cartel affiliated gangs distributing/posting victim data across leak websites belonging to other gangs within the Cartel. In other words, one gang breached and stole data from a victim and passed it to another gang to post publicly and negotiate with the victim.
2. Analyst1 observed multiple gangs within the Cartel coordinating via Cartel leak websites, including sharing tactics, command and control infrastructure, and sharing/posting victim data.
3. Attackers are moving towards automating their attacks. Multiple gangs have added automated capabilities into their ransom payloads, allowing them to spread and infect their victims without human interaction.
4. Ransom demands continue to increase. Collectively, gangs in the Cartel generated hundreds of millions of dollars from ransomware and data extortion operations.
5. Several Cartel gangs offer Ransomware as a Service (RaaS), hiring hackers to execute attacks while providing them with malware, infrastructure, and ransom negotiation services.

6. Attackers are becoming bolder – they are now conducting PR interviews with reporters, issuing press releases, and leveraging social media ads and call centers to harass and pressure victims into paying.
7. Attackers are reinvesting profits made from ransom operations to advance both tactics and malware to increase their success and revenue. Malware is updated regularly, adding new sophisticated features.
8. One gang, Wizard Spider, developed unique malware geared towards espionage. Analyst1 could not validate how Wizard Spider uses it in attacks. It's existence alone is troubling. We found no other gang in the Cartel that uses or develops espionage malware.

Cartel Overview

Four ransomware gangs currently exist within the Cartel: Twisted Spider[2], Viking Spider[3], Wizard Spider[3], and the Lockbit[4] Gang as seen in Figure 1 below.

Figure 1: Cartel Breakdown

Note: The SunCrypt gang is no longer active, but they previously claimed allegiance to the Cartel and have since retired.

The gangs who make up the Cartel originate from eastern Europe and primarily speak Russian, based on posts made to underground criminal forums. Interestingly, all of the gangs build checks and balances into their ransomware to ensure that the payload does not execute on Russian victims. Here, the malware checks if the system language matches a dialect spoken in the Commonwealth of Independent States (CIS), which formerly made up the Soviet Union. Advanced attackers will often even purposely place false flags into their operations to lead investigators astray. However, the Cartel gangs do little to hide the fact they speak Russian, and they go out of their way not to target victims within affiliated Russian territories.

Twisted Spider

During our research into Twisted Spider operations, Analyst1 identified the following key findings associated with the Twisted Spider gang:

- Twisted Spider conducted separate operations using Maze ransomware from May 2019 - November 2020, and they began transitioning to Egregor ransomware from September 2020 to present-day. Each campaign utilized its own malware and infrastructure, primarily separate from one another.
- Twisted Spider created online personas for each campaign, one using Maze and the other Egregor ransomware. The operators who make up the gang use these personas to talk to both the media and security researchers. During media interviews, they discuss their operations and relationships with other ransomware gangs.[5, 6]
- Since its inception, the group has utilized Egregor and Maze ransomware to extort at least $75 million from private sector companies, local governments, and hospitals. We believe this figure to be much more significant, but we can only assess the publicly acknowledged ransom payments. Many victims never publicly report when they pay a ransom.
- Twisted Spider uses a key (string/password) required for the Egregor payload to execute; this makes analysis difficult.
- The gang uses the open-source tool RClone in conjunction with public infrastructure (FTP servers, Dropbox, etc.) to copy and exfiltrate victim data.[7]
- The gang claims to have created a cartel with other well-known ransomware gangs. However they would later attempt to rescind this claim upon retiring their Maze operations and commencing the attacks using the Egregor payload. However, the evidence we discuss in the Cartel Assessment section of this report supports the theory that Twisted Spider and other gangs do work together. Both their retirement and backtracking on the Cartel affiliation after months of promoting it was likely an attempt to throw off researchers and law enforcement.

Viking Spider

Viking Spider first began ransom operations in December 2019. The gang uses ransomware known as Ragnar Locker to compromise and extort organizations. Below are key findings identified while researching Viking Spider activity.

- Viking Spider is the first ransomware attacker to install their own virtual machine (VM) into victim environments to evade detection; they also use it as a launch point to execute the attack.[8]
- The gang is the first to use Facebook ads to pressure victims into paying the ransom.[9]

- Viking Spider outsources call centers in India to contact victims asking them to pay the ransom or risk data exposure. [9]
- Viking Spider uses MSP software to deliver malware and hacktools as well as provide remote access into victim environments.[10]
- Viking Spider is one of the few gangs who conduct DDoS attacks in addition to ransom attacks to pressure victims to pay. A different cartel gang first used this tactic, but Viking Spider quickly adopted it.

Wizard Spider

Wizard Spider is the most experienced attacker within the Cartel. The gang began ransom operations in August 2018, and they are connected to other criminal operations dating back to as early as 2016. Analyst1 identified these key findings during our research into Wizard Spider:

- Wizard Spider has conducted ransom operations previously using Gogalocker and MegaCortex ransomware variants (both of which are now retired), and they currently perform attacks with Ryuk and Conti Ransomware.
- The gang works in multiple teams, conducting simultaneous operations with different ransom payloads. Additionally, they have more malware and hacktools than any other gang associated with the Cartel.
- Wizard Spider developed unique malware geared towards espionage known as Sidoh malware. Analyst1 could not validate how Wizard Spider uses Sidoh in attacks; however, its existence alone is troubling. We found no other gang in the Cartel which uses or develops espionage malware.[11]
- Conti Ransomware uses 32 CPU threads at once to defeat defenses and encrypt data – much faster than any other variant.
- As of February 2021, Ryuk Ransomware includes a new Wake-on-LAN capability, which allows it to automatically discover and spread to victim systems in the target environment.[12]

The Lockbit Gang

The Lockbit Gang first came onto the enterprise ransomware scene in September 2020. Much like the other gangs discussed so far, Lockbit brings its own unique tactics to the ransomware game. Analyst1 found the following findings while researching the Lockbit Gang:

- The Lockbit Gang was the first to automate attacks and remains the most efficient attacker associated with the Cartel.

- Lockbit ransomware uses a self-propagation technique. Upon execution, it issues an ARP request to identify devices within the environment and connects using the SMB protocol to spread.[13] Once connected to a live host, it executes a PowerShell command that connects to attacker C&C infrastructure and downloads the ransom payload (often disguised as an image file).[14]
- At least once, the attacker overwrote the Master Boot Record (MBR) requiring a password to boot. The Lockbit Gang achieved this through the use of the open-source tool BCDedit. BCDedit is a command-line tool that can edit the boot configuration in MS Windows operating systems.[15]

  The Lockbit Gang conducts interviews about their attacks with news media.

The SunCrypt Gang

The SunCrypt gang began conducting ransomware attacks in October 2019. Analyst1 researched the attacks and progression of SunCrypt operations up to present day and found the following key findings:

- SunCrypt is the first gang to introduce denial of service attacks as an extortion tactic used in conjunction with enterprise ransomware attacks.
- The SunCrypt Gang claimed affiliation with both Twisted Spider and the Cartel. Twisted Spider disputed both claims in an interview with Bleeping Computer.[16]
- SunCrypt ransomware uses the Cha Cha 20 stream cipher found in both Twisted Spider's Maze and Egregor ransomware payloads.
- The SunCrypt Gang's ransomware communicated with two C&C IP addresses which Twisted Spider previously used by in their Maze ransomware operations. These findings are significant, since Twisted Spider disputes the SunCrypt Gang's Cartel affiliation claim.
- Operations ceased in October 2020, but transfers from bitcoin wallets funded by victims continue until November 2020.

Cartel Assessment

In November 2020, Twisted Spider – the gang who began the Cartel – announced they were shutting down their operations. In a further twist, they also claimed the Cartel never existed! In their last press release, Twisted Spider stated the Cartel was only real in journalists' minds[17]. Based on the events detailed in our white paper and the specific ties between gangs within the Cartel (outlined next), Twisted Spider's claims are untrue.

The initial claim the gang was retiring was misleading. The tactics used in the attacks overlap in infrastructure, and the technical similarities between Egregor and Maze ransomware made for strong attribution. Clearly, Twisted Spider was behind both operations. The second claim stating the Cartel never existed was not as clear-cut.

Twisted Spider, Viking Spider, Wizard Spider, the Lockbit gang, and the SunCrypt gang claimed they were a ransomware Cartel. Why would all of these criminal gangs speak out publicly, stating they had joined together? To further assess, Analyst1 looked to the evidence to make our own assessment.

The first tie we found provided evidence that the groups are working together and sharing resources to extort victims. Several gangs compromised and stole victim data, which they passed on to Twisted Spider. Twisted Spider then posted the victim's data and attempted to negotiate a ransom on their data leak site. This type of collaboration and sharing would not occur unless all three criminal elements had a trusted relationship with one another. Figure 2 below is a visualization detailing several ties, which we discuss next.

Figure 2:Cartel Ties A & B

Tie A: Shared Victim Data & leak sites

In May 2020, Viking Spider compromised MJ Brunner of brunnerworks.com. After the compromise, Viking Spider posted Brunner's data to their leak site, ragnerleaks[.]top. A few weeks later in June 2020, Twisted Spider posted Brunner data on Viking Spider's behalf along with threatening messages to their data leak site, mazenews[.]top. Not long after, a similar situation took place. This time, the Lockbit Gang breached and attempted to extort a target: the Smith Group. At the time however, the Lockbit Gang did not have a data leak site. In a continued effort to share Cartel resources, Twisted Spider posted the stolen data to their

site, mazenews[.]top, on behalf of the Lockbit gang. Furthermore, Twisted Spider referenced both the Cartel and each member gang who originally stole the data on both occasions. Figure 3 shows the posts below:

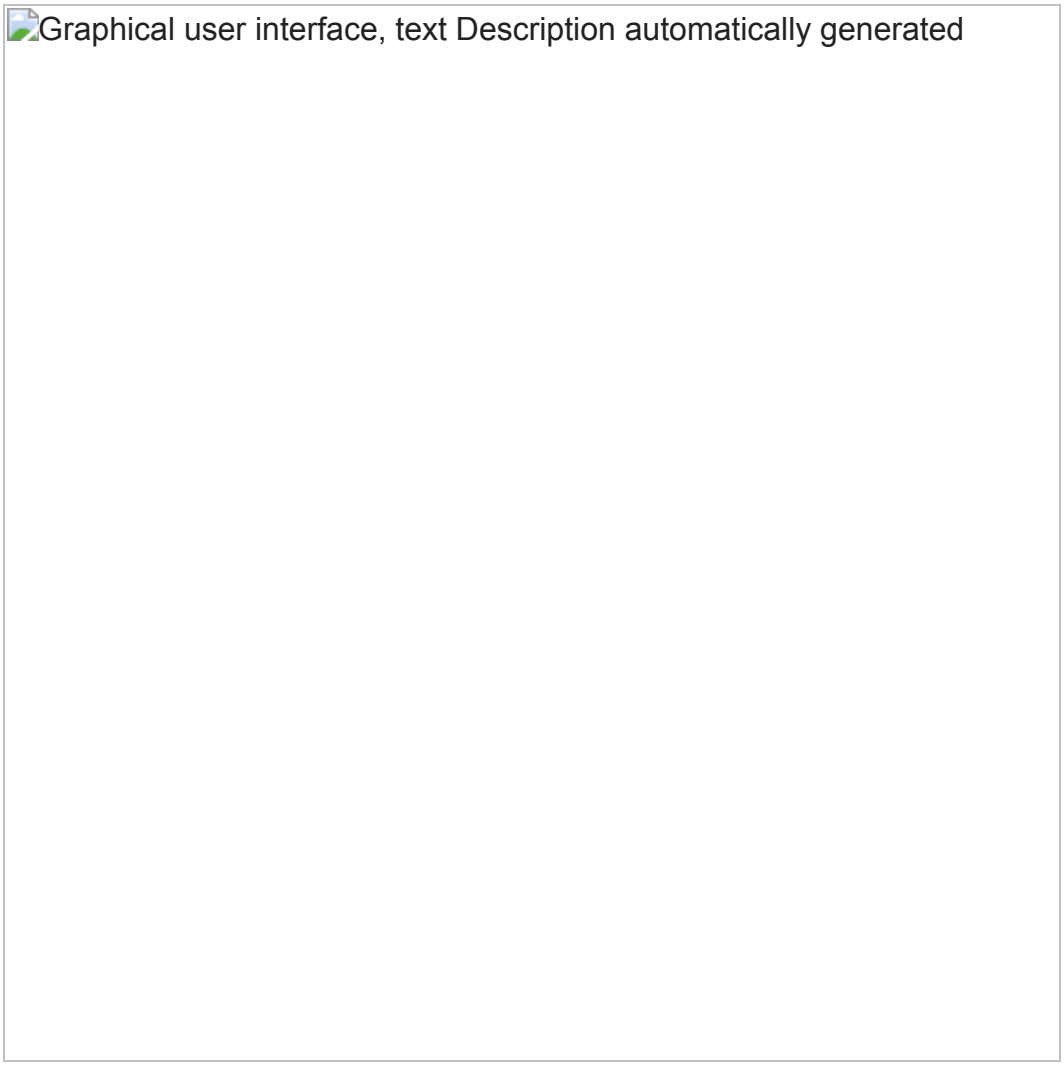


Figure 3: Twisted Spiders data leak site, Mazenews[.]top displaying data stolen by Viking spider (Ragnar) and Lockbit gang.[2, 3]

Tie B: Shared Infrastructure

We mentioned previously that the SunCrypt Gang told Bleeping Computer in August 2020 that they joined the Cartel, which Twisted Spider disputed. Yet, beginning in October 2020 in their early operations, Twisted Spider used two IP addresses, 91.218.114[.][30, 31] for command-and-control infrastructure.[29, 30] Ten months later, the SunCrypt Gang used the same IP addresses for command-and-control to deliver ransomware in their attacks. Granted, the tie would be stronger if the IP used in ransom operations took place during the same time frame. However, Twisted Spider used the 91.218.114.3X range for attacks over at least six months. The extended use and address range indicates that this was persistent

infrastructure that Twisted Spider frequently used and controlled themselves. It is unlikely that the SunCrypt Gang would have access to the infrastructure if they did not have a trusted relationship with Twisted Spider. Table 1 below details the evidence supporting Tie B.

Sha2 Hash	Ransomware	Affiliation	Date	C&C
91514e6be3f581a77daa79e2a4905dcb df6bdcc32ee0f713599a94d453a26fc1	Maze	Twisted Spider	10/2019	91.218.114.30, 91.218.114.31
E3DEA10844AEBC7D60AE330F2730B7ED 9D18B5EEC02EF9FD4A394660E82E2219	SunCrypt	SunCrypt gang	08/2020	91.218.114.30, 91.218.114.31

Table 1: Shared IP space used as C&C for both Twisted Spider and the SunCrypt gang

Other Ties:

Several other circumstantial and technical ties exist as well. These are weaker ties, and you should not use them for attribution on their own. Collectively, however, they are worth discussing:

- Maze and Egregor ransomware (Twisted Spider) and SunCrypt ransomware (SunCrypt Gang) use the Cha Cha stream cypher to encrypt data.
- All of the gangs build checks and balances into their ransomware to ensure the payload does not execute on Russian victims.
- Gangs in the Cartel share and adapt each other's tactics:
  - Double extortion technique (data theft and data encryption)
  - DDoS in conjunction with data theft and data encryption
  - Use of VM within victim environments to execute attacks and avoid detection
  - Use of data leak websites to name and shame
- Additionally, each gang discussed has claimed affiliation to the Cartel. Some of the gangs publicly made these claims to reporters, while others posted on leak sites and social media.

Analyst1 assesses that the Cartel is not an authentic entity, but instead a collective of criminal gangs who, at times, work together in ransom operations. There needs to be more than cooperation, resource, and tactic sharing between gangs for their partnership to qualify as a true Cartel, though. Profit-sharing is the primary element missing in the coalition of ransomware attackers discussed. Cartels are dangerous due to the large financial resources that profit-sharing provides.

Analyst1 researched all known bitcoin wallets and their associated transactions associated with the gangs discussed. We followed the money trail and observed examples of victims paying a gang and gangs paying their affiliates, but we did not find any evidence that the gangs share profits with other gangs in the Cartel.

We believe the gangs created the Cartel facade to appear larger, stronger more powerful to further intimidate victims into paying ransom demands. The illusion and public claims made about the Cartel achieved the desired effect; however, it also brought global attention from

law enforcement and government entities. We believe this prompted Twisted Spider to lie about retiring, and this explains why they attempted to retract their Cartel affiliation. For the same reasons, Twisted Spider stopped communicating publicly, and they no longer use social media or press releases to voice their demands.

Moving forward, Analyst1 believes these ransomware gangs will continue to work with one another. The working relationship, however, will likely continue to be done behind the scenes and not on a public level. Groups will continue to share tactics and resources, making them far more dangerous than if they were operating independently. Both ransomware and malware used to gain initial compromise will increase in their levels of sophistication and capability. Specifically, Analyst1 believes ransomware gangs will focus development efforts to automate attacks. The new capabilities gangs are introducing into their ransomware demonstrate that automation is essential. Analyst1 believes this trend will continue making ransomware operations more efficient and dangerous. As automation capabilities increase, the use of affiliate hackers will decrease. This means ransomware gangs do not have to share profits with affiliates, thus increasing the revenue derived from each attack. With the decrease in the timeframe it takes to execute each attack, Analyst1 believes the overall volume of attacks will grow, raising the number of victims extorted.

Endnotes

1. Infosecurity Magazine. "Police Reportedly Arrest Egregor Ransomware Members" Accessed February 16,2021 https://www.infosecurity-magazine.com/news/police-arrest-egregor-ransomware/

2. CrowdStrike. “Ransomware + Data Leak Extortion: Origins and Adversaries, Pt. 1,” September 24, 2020. https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/.

3. CrowdStrike. "Double Trouble: Ransomware with Data Leak Extortion, Part 2” Accessed March 3, 2021. https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-2/

4. BleepingComputer. "Ransomware gangs team up to form extortion cartel." https://www.bleepingcomputer.com/news/security/ransomware-gangs-team-up-to-form-extortion-cartel/

5. BleepingComputer. “Canon Publicly Confirms August Ransomware Attack, Data Theft.” Accessed March 24, 2021. https://www.bleepingcomputer.com/news/security/canon-publicly-confirms-august-ransomware-attack-data-theft/.

6. BleepingComputer. “SunCrypt Ransomware Sheds Light on the Maze Ransomware Cartel.” Accessed March 24, 2021. https://www.bleepingcomputer.com/news/security/suncrypt-ransomware-sheds-light-on-the-maze-ransomware-cartel/.

7. SentinelLabs. “Egregor RaaS Continues the Chaos with Cobalt Strike and Rclone,” November 25, 2020. https://labs.sentinelone.com/egregor-raas-continues-the-chaos-with-cobalt-strike-and-rclone/.

8. “Ragnar Locker Ransomware Deploys Virtual Machine to Dodge Security.” *Sophos News* (blog), May 21, 2020. https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security/.

9. “Ransomware Group Turns to Facebook Ads — Krebs on Security.” Accessed March 24, 2021. https://krebsonsecurity.com/2020/11/ransomware-group-turns-to-facebook-ads/.

10. BleepingComputer. “Ragnar Locker Ransomware Targets MSP Enterprise Support Tools.” Accessed March 24, 2021. https://www.bleepingcomputer.com/news/security/ragnar-locker-ransomware-targets-msp-enterprise-support-tools/.

11. “2020 Global Threat Report.” Cybersecurity Report. Crowdstrike, 2020. https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf.

12. BleepingComputer. "Ryuk ransomware now self-spreads to other Windows LAN devices." https://www.bleepingcomputer.com/news/security/ryuk-ransomware-now-self-spreads-to-other-windows-lan-devices/

13. “LockBit Ransomware Analysis: Rapid Detonation Using a Single Compromised Credential.” Accessed March 26, 2021. https://www.darktrace.com/en/blog/lock-bit-ransomware-analysis-rapid-detonation-using-a-single-compromised-credential.

14. Gallagher, Sean. “LockBit Uses Automated Attack Tools to Identify Tasty Targets.” Sophos News (blog), October 21, 2020. https://news.sophos.com/en-us/2020/10/21/lockbit-attackers-uses-automated-attack-tools-to-identify-tasty-targets/.

15. The DFIR Report. “Lockbit Ransomware, Why You No Spread?,” June 10 2020. https://thedfirreport.com/2020/06/10/lockbit-ransomware-why-you-no-spread/.

16. BleepingComputer. “SunCrypt Ransomware Sheds Light on the Maze Ransomware Cartel.” Accessed March 26, 2021. https://www.bleepingcomputer.com/news/security/suncrypt-ransomware-sheds-light-on-the-maze-ransomware-cartel/.

17. BleepingComputer. “Maze ransomware shuts down operations, denies creating cartel.” Accessed March 19, 2021. https://www.bleepingcomputer.com/news/security/maze-ransomware-shuts-down-operations-denies-creating-cartel/