How a Texas hack changed the ransomware business forever

By Dina Temple-Raston

Published: 2023-01-17 · Archived: 2026-04-06 03:31:29 UTC

The early morning hours of August 16, 2019 began with the whirring and burping sound of computer printers. The scratch and screech echoed along the empty corridors of the Borger, Tex. administrative offices, paper sliding from tray to ink jet to tray and then back again.

Anyone in the office that steamy Friday who happened to glance at the finished pages would have seen sheets covered in gibberish: all ampersands, exclamation points and broken English.

To Jason Whisler, the city's emergency management coordinator, it was clear what this meant: Borger, population 13,000, was suffering from a ransomware attack and those pages on the printers were filled with demands. "If you read between the lines it basically said, you know, the system's been infected," Whisler recalled. "It was a very definite pay up or else."

Borger wasn't alone; it was one of nearly two dozen cities around the state that woke up that morning to find computers either locked up or misbehaving. They would learn much later that hackers had managed to infiltrate their managed service provider, the company that was handling their IT, and by cracking into the MSP they had their pick of dozens of victims – it was very efficient. And all the cyber criminals wanted to make it stop was $2.5 million in Bitcoin.

"The city manager at the time, he asked me, 'I have to ask because insurance is asking, do we want to consider paying the ransom?" Whisler said. "Immediately I said no." In his view, it was tantamount to negotiating with terrorists.

The decision not to pay had a surprising knock-on effect: it forced a notorious ransomware gang, the Russia-based REvil, or ransomware evil, to rethink how it did business. What it came up with – something called ransomware-as-a-service – is a big part of the reason why ransomware is one of the fastest-growing cybersecurity threats in the world today.

> https://www.youtube.com/watch?v=8p2LeQiQjLI
>
> What does a hack look like in real time? Here are some cyber surveillance videos.

Ransomware-as-a-service, or RaaS, is a franchise model. Instead of launching a ransomware attack from beginning to end, cybercriminals have started to divvy up the work. In REvil's case, it decided to give the time-consuming, front-end reconnaissance work of a hack to other groups: they could unearth vulnerabilities that compromise networks, and REvil would handle everything necessary for the ransomware operation itself from malware packages to negotiators to Bitcoin wallets waiting for payments. For their services, REvil would get a percentage of any ransom money paid.

In an interview published by The Record last year, one REvil manager claimed that the group had developed a coterie of more than 60 affiliates all of whom were launching cyber attacks. So instead of one group holding a couple dozen servers ransom as had happened in the past, there were dozens of groups working simultaneously to lock up tens of thousands of them.

Ransomware evil

About a year before the Texas attack, a managed service provider named Certified CIO discovered it had been compromised. Hackers had infiltrated its client networks and were beginning to take control of their servers in order to hold them for ransom.

“We got called out because they just happened to be local enough to us that we could make the trip and sit alongside an incident response firm,” said Kyle Hanslovan, the CEO of Huntress, a cyber security firm. “And during the process, we realized that the actor got into the remote management software” of the MSP.

It so happens that a videofeed the company had set up to record their help sessions with clients had accidentally captured the bad guys at work. So Hanslovan and his team suddenly had hours and hours of what was essentially cyber surveillance footage. They could see the hackers methodically working their way through the client networks – turning off virus scanners, encrypting each host and stealing their passwords.

“You could actually see them on screen,” Hanslovan said. “What's funny is the naming schemes to the tactics, to the capabilities, to what they checked and what did they do after they got initial access” all provided incredible insight into how the group ran their intrusions and Hanslovan came to believe that a group he’d had an eye on for years, a group that would eventually become REvil, was behind it all.

“My first run-ins with REvil were probably well before they ever called themselves REvil, is probably like 2017. Maybe even as early as 2016,” he said, adding that he recognized them because they loved to target MSPs like Hanslovan’s client, Certified CIO.

The gang, it turns out, were particularly good at finding vulnerabilities in MSP software and at the time they were the only ones that appeared to be doing it. When Hanslovan heard about what happened in Texas, he was pretty sure REvil, the group he had studied for years, was behind that, too.

Manager: Unknown

Last year, a security analyst named Dmitry Smilyanets had a long online chat with someone who claimed to be a member of REvil’s management team. He went by the online handle ‘Unknown.’

“Unknown was not a hacker. He was the operator. He was the manager,” Smilyanets said. “His job was to control the infrastructure, make sure it all works. Make sure that communication lines with victims were up and that payments go through.”

Smilyanets didn’t just take Unknown’s word for it. He had been watching the REvil manager for some time, tracking his message traffic on the dark web, watching as his online wallet swelled with Bitcoin, and Smilyanets eventually became convinced that Unknown was who he claimed to be. (Smilyanets works at Recorded Future, a threat intelligence company. Click Here and The Record are divisions of Recorded Future and are editorially independent.)

While it is impossible to verify all the claims Unknown made in his chat with Smilyanets, he did make clear that after 2019, REvil did some rethinking. “Their main goal is to make money and they will not stop on anything until they make this money,” Smilyanets said. “They bring new tactics, new techniques to help to pressure the victim to pay.”

Ransomware-as-a-service was one of those new techniques. RaaS was not just more efficient, it provided a level of deniability. Security analysts and law enforcement might spot REvil’s code in the ransomware, but because of the new business model, they couldn’t be sure if REvil was actually behind it. What’s more, because REvil was cycling through various affiliate groups it complicated attempts at attribution. According to the Justice Department since 2019, REvil has been linked to some 175,000 ransomware attacks, generating some $200 million in ransom.

“We kind of slept”

For Whisler and Garrett Spradling, Borger’s city manager, the events of 2019 never became a whodunnit. Their singular focus was on getting the city’s computers running again. "I've got enough to deal with the day-to-day business in the city of Borger,” Spradling said. “I mean, as bad as it may or may not sound, I didn't even think about the other cities. I have enough to worry about with my city.”

So the fact that REvil was involved seemed at the time, and even now, beside the point. Chasing cybercriminals was left to others: federal law enforcement, including the FBI and, sometimes, the NSA.

Before Texas, the people behind epic hacks tended to be nation-state actors. The North Koreans broke into Sony Pictures in 2014; the Chinese stole millions of secret personnel files from the Office of Personnel Management a year later. Those kinds were America's main adversaries in cyberspace and they were known as APTs – Advanced Persistent Threats and in attacks against the U.S. they were usually from one of the Big Four: Russia, China, North Korea or Iran.

Kyle Hanslovan used to work at the NSA and he said the focus inside Fort Meade, where the NSA and Cybercom fight these kinds of threats, was almost exclusively on the nation-state variety.

> https://twitter.com/campuscodi/status/1481989170876882944?s=20&t=_JmvNLHqvUEj8sGvQQLQWw

"'Let's go after the ATP' was what it was all about back then," he said. And because there was such a focus on those actors, Hanslovan believes "we kind of slept" through an important shift: in 2015 or 2016, criminals were starting to weaponize cyberspace too. "We were late behind the power curve on all of ransomware-as-a-service," Haslovan said.

The criminal element started slow, with something called initial access brokers – just run-of-the-mill hackers who found vulnerabilities in random computers and bundled them together. "Initial access brokers would get people who have all these unimportant accesses to computers and bundle them together, and resell them for dirt cheap," said Hansolvan. "We're talking about sometimes as cheap as $10 for access."

The buyers would root around the various access points to see where it might take them. Could a small vulnerability on one computer, for example, allow them to monkey bar over to something else – like a company email system or a company network? If that happened, they figured out that that access they bought for $10 could now be sold for $100 – maybe even $1,000..

It was a service model.

"You could have looked circa 2018 and seen that this behavior was going to happen," Hanslovan said. "It just made economical sense. It's the same reason, again, that you have somebody delivering your paper for the last mile. It just makes so much sense to have a one-to-many relationship, but we were kind of very slow as a [cybersecurity] culture to react to it."

A $44,000 bill

Borger might have emerged from that 2019 attack as just another victim had they not been in the middle of upgrading their servers. It happened to have been in the middle of transferring its data over to a new City Hall server that August. Then Mother Nature lent a hand.

"By luck, we had a faulty ups with that server," Whisler said. "And a couple of nights before we had some storms roll through and when the power flickered that server shut down and was also offline. So even though a lot of our

individual desktops were affected by this through the network, the lion's share of our data that we need for just city operations, utility billing, that was actually preserved on a server that had shut down."

Spradling, the city manager, said that and a couple of other happy accidents meant that the ransomware attack was scary, but in the end not all that costly. To make everything right again ran the city about $44,000, he said, which wasn't even half the city's general contingency funding. The State of Texas helped them too. Officials talked to some of the computer companies, explained what happened, and the companies gave Borger a huge discount on new computers Whisler said they needed to upgrade anyway.

"It's satisfying that they didn't get anything," he said. "Our overall expenses are our losses and the replacement was mitigated by the state and we didn't pay any of the ransom. So all in all, I would call it a successful failure."

In its own way, REvil probably saw it that way too until back in October when their luck seemed to run out: U.S. Cyber Command and the NSA launched an offensive cyber operation against REvil, Reuters reported. They took over their server and redirected all their traffic, basically shuttering their RaaS ransomware operation.

A few months later, Moscow fired its own salvo. It released a video of authorities raiding the homes of more than a dozen alleged REvil members. Moscow said afterward it arrested REvil members as a favor to President Biden.

As for the REvil manager, Unknown, he has been missing for months. "He's disappeared," Smilyanets said.

And at least for now, REvil has too.

— *Additional reporting by Sean Powers and Will Jarvis*

> https://www.scribd.com/document/557499558/Click-Here-Ep-1-How-a-Texas-hack-changed-the-ransomware-business-forever-Transcript

No previous article

No new articles

Dina Temple-Raston

is the Host and Managing Editor of the Click Here podcast as well as a senior correspondent at Recorded Future News. She previously served on NPR's Investigations team focusing on breaking news stories and national security, technology, and social justice and hosted and created the award-winning Audible Podcast "What Were You Thinking."
