Taking the Fight to the Ransomware Gangs: The Impact on Law Firms

By Sharon D. Nelson, Esq., John W. Simek and Michael C. Maschke

Going on the Offensive: A New Development in Combatting Ransomware

For as long as ransomware gangs have been around, we've been rocked back on our heels in defensive mode. No longer. Following the old adage about taking the fight to the enemy, we have set out to make it painful to be in a ransomware gang. We have taken the gloves off in our quest to disrupt the cyber criminals.

Who is Fighting Ransomware?

Everyone knew that, under the Biden administration, cybersecurity was a priority – one of the few things that both political parties could agree upon. Notable has been the elevation of the Cybersecurity and Infrastructure Security Agency (CISA), which is part of the Department of Homeland Security. CISA has risen to great prominence producing all sorts of resources, one of them noteworthy for this article. The resource is Stop Ransomware, a site full of helpful advice in plain English found at https://www.cisa.gov/stopransomware.

But what we didn't know until December of 2021 was that the U.S. military is taking on ransomware as well, particularly worried about attacks on critical infrastructure. Mind you, the military doesn't want to tell us exactly what it is doing which is unsurprising. General Paul M. Nakasone, the head of the US Cyber Command and director of the National Security Agency, has said that one of the goals of the current operations is to "impose costs" for ransomware groups.

We have also added private companies to the fight, including Amazon, Google and Microsoft. CISA is teaming with private companies in the Joint Cyber Defense Collaborative, which will focus first on combatting ransomware and attacks on cloud providers – concurrently working on information sharing between the government and the private sector.

The Department of Justice Had a Very Good Month in November 2021

In a series of moves, the DOJ sent ransomware gangs a strong message. It arrested a REvil affiliate in Poland to be extradited to the U.S.

It seized $6.1 million in cryptocurrency from another REvil associate.

Finally, it offered a bounty of $10 million for the name or location of any key REvil leader and up to $5 million for information about REvil affiliates. That's some serious money!

January 2022: The Russians Say They Shut Down REvil with Information Provided by the U.S.

Eyebrows no doubt went up everywhere when that news was reported. The Federal Security Service (FSB) of the Russian Federation announced that REvil was now shut down and "the information infrastructures used for criminal purposes was neutralized."

Fourteen REvil members were arrested, apparently based on information provided by the U.S.

Russian authorities confiscated cryptocurrency and fiat money, including more than 426 million rubles (approximately $5.5 million), 600 thousand U.S. dollars and 500 thousand euros (approximately $570,000).

They also confiscated 20 luxury cars purchased with money obtained from cyberattacks, computer equipment and cryptocurrency wallets used to develop and maintain the ransomware operation.

Chatter on the Dark Web: The Criminals are Worried

Not surprisingly, members of ransomware gangs are worried about being tracked down and arrested. They expressed in their dark web chatter that they had no desire to go to jail (imagine that). Previously, jail had never seemed a possibility as Russia turned a blind eye to the activities of ransomware gangs.

Some mentioned moving out of Russia. Others worried that criminals who are arrested will rat out their comrades. That seems likely. Suddenly, there was a ripple of fear pervading in the ransomware cartels that didn't exist before. Crime may indeed have consequences.

What Do Recent Developments Portend for the Longstanding Battle of Law Firms Against Ransomware?

It is hard to know this early on how law firms may be impacted by the recent victory against REvil. Bear in mind that the Russian cooperation may have much to do with diplomacy. It may have been a good moment to give the Americans something they wanted (Russia doing something about the many ransomware gangs it harbors) while plans to attack Ukraine were clearly underway.

Also, a new ransomware group has popped up called the "Ransom Cartel." DataBreachToday reported on January 24 that "Security experts say the new group has technical and other crossovers with REvil. But whether the new group is a spinoff of REvil, bought the tools, or is simply copying how they work, remains unclear." As we have always said, shutting down ransomware gangs amounts to playing a game of "whack-a-mole."

Law firms are still being attacked every day. We know that because of what we do for a living. But the actions we've seen taken in the U.S. are significant – and over time, they may have their intended effect, disrupting the gangs through arrests, siphoning their cryptocurrency, etc. The clear advice for law firms is "don't let your guard down."

Law firms are still, as Forbes once noted, a great "one stop shopping" way to get the data of many corporations, government entities, etc. They remain the crown jewel prize for ransomware gangs, so while we applaud the commendable actions taken thus far, the war against ransomware is far from over. In many ways, it has just begun.

Sharon D. Nelson *is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA.* *snelson@senseient.com*

John W. Simek *is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH) and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm.* *jsimek@senseient.com.*

Michael C. Maschke *is the CEO/Director of Cybersecurity and Digital Forensics of Sensei Enterprises, Inc. He is an EnCase Certified Examiner, a Certified Computer Examiner (CCE #744) a Certified Ethical Hacker and an AccessData Certified Examiner. He is also a Certified Information Systems Security Professional.* *mmaschke@senseient.com.*