Unraveling How Cybercriminals Extort Businesses Worldwide

Research finds that criminal organizations are highly sophisticated, often acting like corporate franchisees

AUGUST 29, 2022

Finance

Over the years, Fuqua School of Business finance professor Campbell Harvey has published hundreds of papers and testified before government committees about a wide range of economic issues. But until a recent paper on cybercrimes, he never felt his work might put him in peril.
The paper, "An Anatomy of Crypto-Enabled Cybercrimes," takes a detailed look at how highly sophisticated criminal organizations, mainly based in Russia and North Korea, extort money from corporations worldwide. The majority of these victimized firms are in the United States.

"This was actually a difficult decision to do this paper because there's a substantial probability that I will be targeted," Harvey said. "But we want academics to do basic research like this because it is important that policymakers make the right decisions" regarding cryptocurrency, such as bitcoin.

"We believe the insights we've provided will help policymakers make nuanced decisions about cryptocurrency, which has a number of positive benefits, such as promoting financial inclusion, reducing transaction costs, and providing new capital for startups," Harvey added.

But the risks associated with cyber criminals can also be great, as was seen last year when cybercriminals disrupted gas distribution in the eastern U.S. by successfully hacking Colonial Pipeline. More broadly, cybercriminals extorted a record $14 billion in cryptocurrency in 2021, a 79% increase over the previous year, according to the blockchain analytics firm Chainalysis.

It took more than a year for Harvey, his three co-authors and their research team to gain an understanding of how these criminal organizations operate. To do so, they mined a diverse set of public, proprietary, and hand-collected data, including dark web conversations in Russian, and used blockchain forensics and other investigative tools.

Harvey said he was surprised to discover that the criminal organizations operate at such a refined level.

"This is not a lone operator who happens to get lucky. This is highly sophisticated, a corporate-like operation," with physical offices, call centers and investments in blockchain technology, and other decentralized finance (DeFi) tools, to launder the attack proceeds, he said.

The biggest ransomware gangs function as umbrella organizations that then provide to smaller hacker groups the software needed to successfully overtake a company’s computer system, Harvey said. When a smaller group successfully collects a ransom, it pays the umbrella group a 15% royalty, similar to how corporate franchises operate.

Another surprise, Harvey said, was that cybercriminals typically keep their word to unlock a company’s computer system once a ransom is paid. "Ransomware gangs also value reputation, a feature that victims can leverage to contain the damages of a ransomware attack," the paper notes.

In the paper, the authors provide a real-life example of a hacker-victim negotiation:

Victim: "Can you please tell us what we will receive once payment is made?"

Attacker: "You will get: 1) full decrypt of your systems and files 2) full file tree 3) we will delete files which we taken from you 4) audit of your network."
Victim: This situation is very difficult for us and we are worried we may get attacked again or pay and you will still post our data. What assurances or proof of file deletion can you give us?

Attacker: "We have reputation and word, we worry about our reputation as well. After successful deal you will get: 1) full file trees of your files 2) after you will confirm we will delete all information and send you as proof video. We are not interested in to give to someone other your own data. We never work like that."

Harvey said the criminals continue to add new layers of extortion, making hacks harder to detect and fight off. But he added that many companies have not done nearly enough to protect themselves from such attacks, and often hide from the public that they have been victimized.

"This is a first-level risk within the firm, but many companies don’t treat it as such, so they underinvest in cybersecurity measures. They treat it as an IT problem rather than a strategic risk."

Rather than blanket restrictions on cryptocurrency, Harvey and his co-authors write that blockchain transparency and digital footprints enable effective forensics for tracking, monitoring, and shutting down dominant cybercriminal organizations.

"A one-size-fits-all solution, such as restricting or banning cryptocurrency usage by individuals or organizations, is problematic for three major reasons," the paper says. "First, this is not a national problem. Blockchains exist across multiple countries and harsh regulations in a particular country or jurisdiction have little or no effect outside that country. As we have seen from other global initiatives (e.g., carbon tax proposals), it is nearly impossible to get global agreement.

"Second, while an important problem, cryptocurrency plays a small role in the big picture of illegal payments. Physical cash is truly anonymous and, indeed, this may account for the fact that 80.2% of the value of U.S. currency is in $100 notes. It is rare that consumers use $100 bills and it is equally rare that retailers are willing accept them.

"Third, and most importantly, expunging all cryptocurrency use in a country eliminates all of the benefits of the new technology. Further, it puts the country at a potential competitive disadvantage. For example, a ban on crypto effectively eliminates both citizens and companies from participating in web3 innovation."

The authors say regulators need to take advantage of the fact that all transactions using blockchain technology are viewable. "This opens the possibility of deploying forensic tools with a focus on tracking, monitoring and identifying the crypto transactions attributed to criminals," the authors write.

Contact Info

For more information contact our media relations team at media-relations@fuqua.duke.edu.