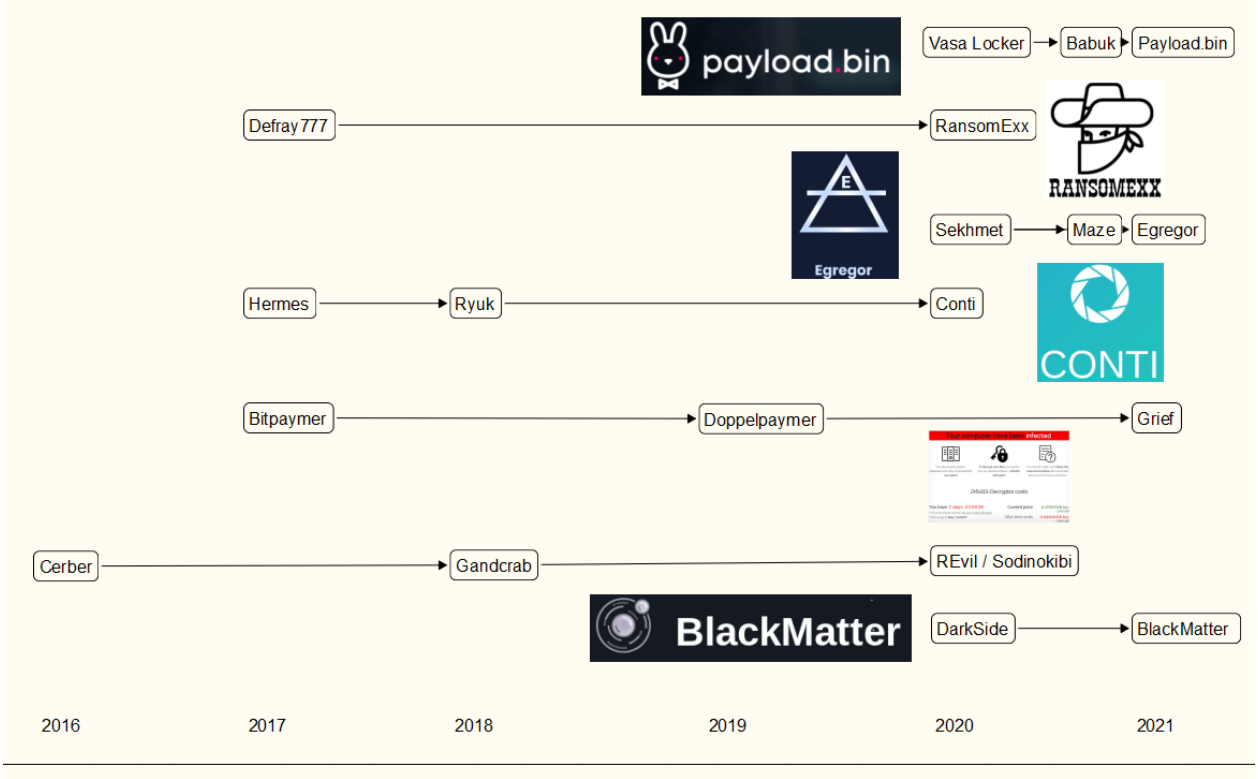
Ransomware Gangs and the Name Game Distraction

krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/

It's nice when ransomware gangs have their bitcoin stolen, malware servers shut down, or are otherwise forced to disband. We hang on to these occasional victories because history tells us that most ransomware moneymaking collectives don't go away so much as reinvent themselves under a new name, with new rules, targets and weaponry. Indeed, some of the most destructive and costly ransomware groups are now in their third incarnation.



A rough timeline of major ransomware operations and their reputed links over time.

Reinvention is a basic survival skill in the cybercrime business. Among the oldest tricks in the book is to fake one's demise or retirement and invent a new identity. A key goal of such subterfuge is to throw investigators off the scent or to temporarily direct their attention elsewhere.

Cybercriminal syndicates also perform similar disappearing acts whenever it suits them. These organizational reboots are an opportunity for ransomware program leaders to set new ground rules for their members — such as which types of victims aren't allowed (e.g., hospitals, governments, critical infrastructure), or how much of a ransom payment an affiliate should expect for bringing the group access to a new victim network.

I put together the above graphic to illustrate some of the more notable ransom gang reinventions over the past five years. What it doesn't show is what we already know about the cybercriminals behind many of these seemingly disparate ransomware groups, some of whom were pioneers in the ransomware space almost a decade ago. We'll explore that more in the latter half of this story.

One of the more intriguing and recent revamps involves **DarkSide**, the group that extracted a $5 million ransom from **Colonial Pipeline** earlier this year, only to watch much of it get clawed back in an operation by the U.S. Department of Justice.

After acknowledging someone had also seized their Internet servers, DarkSide announced it was folding. But a little more than a month later, a new ransomware affiliate program called **BlackMatter** emerged, and experts quickly determined BlackMatter was using the same unique encryption methods that DarkSide had used in their attacks.

DarkSide's demise roughly coincided with that of **REvil**, a long-running ransomware group that claims to have extorted more than $100 million from victims. REvil's last big victim was **Kaseya**, a Miami-based company whose products help system administrators manage large networks remotely. That attack let REvil deploy ransomware to as many as 1,500 organizations that used Kaseya.

REvil demanded a whopping $70 million to release a universal decryptor for all victims of the Kaseya attack. Just days later, **President Biden** reportedly told Russian **President Vladimir Putin** that he expects Russia to act when the United States shares information on specific Russians involved in ransomware activity.

A REvil ransom note.

Whether that conversation prompted actions is unclear. But REvil's victim shaming blog would disappear from the dark web just four days later.

Mark Arena, CEO of cyber threat intelligence firm Intel 471, said it remains unclear whether BlackMatter is the REvil crew operating under a new banner, or if it is simply the reincarnation of DarkSide.

But one thing is clear, Arena said: "Likely we will see them again unless they've been arrested."

Likely, indeed. REvil is widely considered a reboot of GandCrab, a prolific ransomware gang that boasted of extorting more than $2 billion over 12 months before abruptly closing up shop in June 2019. "We are living proof that you can do evil and get off scot-free," Gandcrab bragged.

And wouldn't you know it: Researchers have found GandCrab shared key behaviors with **Cerber**, an early ransomware-as-a-service operation that stopped claiming new victims at roughly the same time that GandCrab came on the scene.

GOOD GRIEF

The past few months have been a busy time for ransomware groups looking to rebrand. *BleepingComputer* recently reported that the new "**Grief"** ransomware startup was just the latest paintjob of **DoppelPaymer**, a ransomware strain that shared most of its code with an

earlier iteration from 2016 called **BitPaymer**.

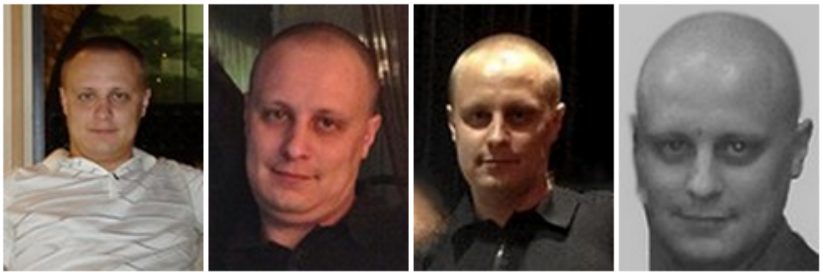
All three of these ransom operations stem from a prolific cybercrime group known variously as TA505, "**Indrik Spider**" and (perhaps most memorably) **Evil Corp**. According to security firm **CrowdStrike**, Indrik Spider was formed in 2014 by former affiliates of the GameOver Zeus criminal network who internally referred to themselves as "The Business Club."

The Business Club was a notorious Eastern European organized cybercrime gang accused of stealing more than $100 million from banks and businesses worldwide. In 2015, the FBI offered a standing $3 million bounty for information leading to the capture of the Business Club's leader — **Evgeniy Mikhailovich Bogachev**. By the time the FBI put a price on his head, Bogachev's Zeus trojan and later variants had been infecting computers for nearly a decade.

WANTED
BY THE FBI

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering

EVGENIY MIKHAILOVICH BOGACHEV



Multimedia: Images

Aliases:
Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoon"

DESCRIPTION

Date(s) of Birth Used:	October 28, 1983	**Hair:**	Brown (usually shaves his head)
Height:	Approximately 5'9"	**Eyes:**	Brown
Weight:	Approximately 180 pounds	**Sex:**	Male
NCIC:	W890989955	**Race:**	White
Occupation:	Bogachev works in the Information Technology field.		

Remarks: Bogachev was last known to reside in Anapa, Russia. He is known to enjoy boating and may travel to locations along the Black Sea in his boat. He also owns property in Krasnodar, Russia.

The alleged ZeuS Trojan author, Evgeniy Mikhaylovich Bogachev. Source: FBI

Bogachev was way ahead of his colleagues in pursuing ransomware. His Gameover Zeus Botnet was a peer-to-peer crime machine that infected between 500,000 and a million **Microsoft Windows** computers. Throughout 2013 and 2014, PCs infected with Gameover were seeded with Cryptolocker, an early, much-copied ransomware strain allegedly authored by Bogachev himself.

CrowdStrike notes that shortly after the group's inception, Indrik Spider developed their own custom malware known as Dridex, which has emerged as a major vector for deploying malware that lays the groundwork for ransomware attacks.

“Early versions of Dridex were primitive, but over the years the malware became increasingly professional and sophisticated,” CrowdStrike researchers wrote. “In fact, Dridex operations were significant throughout 2015 and 2016, making it one of the most prevalent eCrime malware families.”

That CrowdStrike report was from July 2019. In April 2021, security experts at **Check Point Software** found Dridex was still the most prevalent malware (for the second month running). Mainly distributed via well-crafted phishing emails — such as a recent campaign that spoofed **QuickBooks** — Dridex often serves as the attacker’s initial foothold in company-wide ransomware attacks, CheckPoint said.

REBRANDING TO AVOID SANCTIONS

Another ransomware family tied to Evil Corp. and the Dridex gang is **WastedLocker**, which is the latest name of a ransomware strain that has rebranded several times since 2019. That was when the Justice Department put a $5 million bounty on the head of Evil Corp., and the Treasury Department’s **Office of Foreign Asset Control** (OFAC) said it was prepared to impose hefty fines on anyone who paid a ransom to the cybercrime group.

Alleged Evil Corp leader Maksim “Aqua” Yakubets. Image: FBI

In early June 2021, researchers discovered the Dridex gang was once again trying to morph in an effort to evade U.S. sanctions. The drama began when the Babuk ransomware group announced in May that they were starting a new platform for data leak extortion, which was intended to appeal to ransomware groups that didn't already have a blog where they can publicly shame victims into paying by gradually releasing stolen data.

On June 1, Babuk changed the name of its leaks site to payload[dot]bin, and began leaking victim data. Since then, multiple security experts have spotted what they believe is another version of WastedLocker dressed up as payload.bin-branded ransomware.

"Looks like EvilCorp is trying to pass off as Babuk this time," wrote **Fabian Wosar**, chief technology officer at security firm **Emsisoft**. "As Babuk releases their PayloadBin leak portal, EvilCorp rebrands WastedLocker once again as PayloadBin in an attempt to trick victims into violating OFAC regulations."

Experts are quick to point out that many cybercriminals involved in ransomware activity are affiliates of more than one distinct ransomware-as-a-service operation. In addition, it is common for a large number of affiliates to migrate to competing ransomware groups when their existing sponsor suddenly gets shut down.

All of the above would seem to suggest that the success of any strategy for countering the ransomware epidemic hinges heavily on the ability to disrupt or apprehend a relatively small number of cybercriminals who appear to wear many disguises.

Perhaps that's why the Biden Administration said last month it was offering a $10 million reward for information that leads to the arrest of the gangs behind the extortion schemes, and for new approaches that make it easier to trace and block cryptocurrency payments.