France’s lead cybercrime investigator on the Egregor arrests, cybercrime

March 16, 2021

Catalin Cimpanu
March 16, 2021

For more than half a decade, ransomware gangs have operated with impunity and have generally avoided the long arm of the law, with very few of the perpetrators facing consequences for their destructive attacks.

We’ve seen hundreds of ransomware operations, but only a handful of arrests, such as those involving the creators of the CoinVault ransomware or distributors for the GandCrab, NetWalker, and CTB-Locker & Cerber ransomware.

However, last month, we’ve seen one of the most successful crackdowns against a ransomware operation to date, when in a joint investigation, French and Ukrainian authorities were able to track down and arrest three members of the Egregor ransomware cartel.

The arrests, which took place across Ukraine, were the result of an investigation that began in France after a series of attacks by the Egregor gang against French companies like Ubisoft, Gefco, and Ouest France.

Leading the Ukrainian operation of the investigation was **François B.**, the Head of the Computer Security Incident Response Team for the French Judicial Police (CSIRT-PJ), who leads teams of IT and security professionals embedded with French police with the sole purpose of aiding their investigations with technical expertise.

Below is an email interview the French police official agreed to grant The Record this month, albeit with the caveat that some details couldn't be shared in full due to a still-ongoing investigation into the Egregor gang's operations. The interview has been lightly edited for grammar.

The Record: French police made headlines last month after its partnership with Ukrainian police resulted in the arrest of several suspects believed to be involved with the Egregor ransomware cartel. Without revealing sensitive details about the ongoing case, can you tell us what led to your decision to target this specific group?

François B.: We do not share operational MO, but let's say our Ukrainian partners and us had pieces that added up.

TR: Two security firms told The Record that following the arrests, they had not seen any new cases of Egregor attacks. Do you believe that you arrested the main culprits who operated the service?

FB: A little bit of both. One of them seemed to be deeply involved with the main actor and had access to the most critical resources. The other two were providing support (privilege escalation, for instance).

TR: Will we see new cases spawning from the Egregor arrest? Have you and your Ukrainian partners been able to retrieve more data about other Egregor affiliates?

FB: Investigation is still ongoing.

TR: Despite ransomware attacks being such a huge issue for both the public and private sector, until now, only members of the Netwalker and Egregor gangs have been arrested. Why do you think law enforcement, in general, is having such a hard time tracking down ransomware gangs, as opposed to other forms of cybercrime?

FB: Ransomware infrastructure is often elaborate and extensive. When you add the judiciary's complexity, the investigation is not as fast and reactive for investigators as for perps.

TR: In your role as Head of the Cyberintelligence Division at CSIRT-PJ, what is the typical process in tracking down suspects of cybercrime offenses?

FB: We map infrastructure with IOCs [indicators of compromise] found on infected devices provided by investigators and give them new tracks to work on (usually servers to seize, intercept, copy). We are a technical support unit working for investigators enforcing CSIRT's procedures for IR [incident response] and intelligence management.

> Ransomware infrastructure is often elaborate and extensive. When you add the judiciary's complexity, the investigation is not as fast and reactive for investigators as for perps."
>
> *— François B., Head of the Computer Security Incident Response Team for the French Judicial Police*

TR: Over the past few years, Dutch Police have built a reputation of mercilessly going after cybercrime groups that operate inside their borders. Is this something French Police is aiming for in the long term — to make criminals afraid of hosting infrastructure in France or targeting French users?

FB: French police are obviously protecting French citizens, but our main goal is to have a broader perspective and to have the cybercriminals arrested and prosecuted.

TR: What are the biggest problems your department has encountered when investigating and tracking down cybercrime operators?

FB: We are gaining in maturity, which is a slow but very interesting process. Resources (manpower and skills) are also mandatory.

TR: What are your department's strongest skillsets in combating cybercrime?

FB: Since our engineers are embedded in a police department, we try to have the best fit with the investigators' mindset and to take advantage of both worlds: technical and police.

TR: Private-public sector partnerships in the cybersecurity space have evolved over the past few years. Does the French Police maintain such partnerships?

FB: Yes, we maintain such partnerships with incident response companies like Orange Cyberdefense, Wavestone, TrendMicro for AV, Linkurious for data analysis, Serenicity (detection), Signal Spam, or Phishing initiative.

TR: How have these partnerships improved your work on active investigations? Any specific tools or external services that you found more useful than others?

FB: They provide us with the most accurate information on an ongoing case, tools, or threat intelligence data.

TR: Do you investigate APT (state-sponsored hacking) operations as well?

FB: Our job is focused on cybercrime; state-owned attacks are handled by other services.

TR: Security firms often release reports about the most dangerous cyber threats and trends. However, it's law enforcement agencies that often see the real and actual trends of the cybercrime ecosystem. What are the types and forms of cybercrime your agency is usually dealing with?

FB: Our main victim provider is ransomware. We also see a lot of phishing and fraud.

TR: You've been with the CSIRT-PJ team for more than five years now. Are there any past cases that stand out in your career the most that you usually remember as some of your team's best achievements?

FB: Our first case, a RAT sent to a bank. We managed to OSINT the bad guy's room on Google Street View.

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.