GandCrab ransomware distributor arrested in South Korea

By Catalin Cimpanu

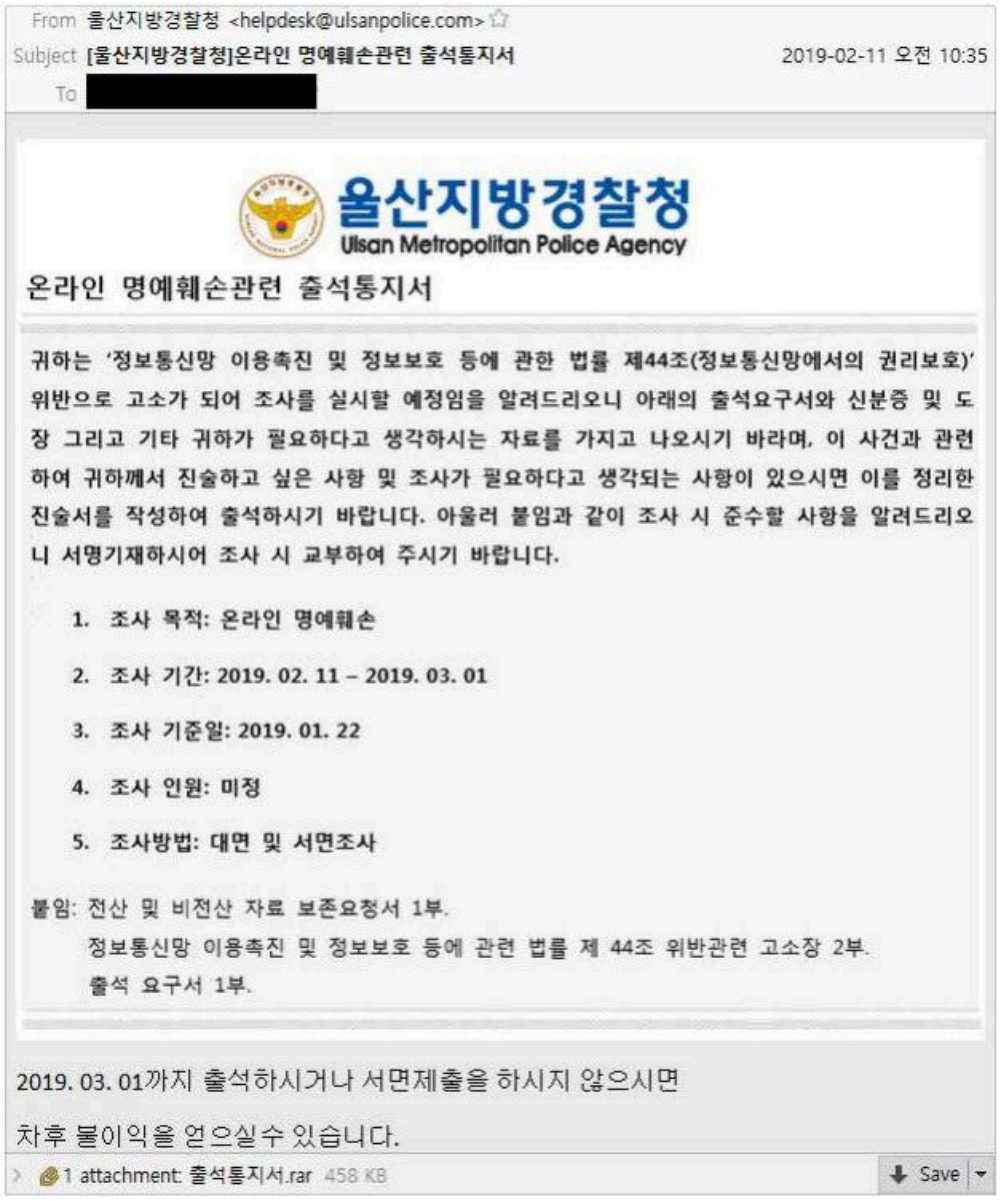
Published: 2022-11-17 · Archived: 2026-04-06 00:20:25 UTC

South Korean national police have announced today the arrest of a 20-year-old suspect on charges of distributing and infecting victims with the GandCrab ransomware.

The suspect, whose name was not released, operated as a customer of the GandCrab Ransomware-as-a-Service (RaaS) cybercrime operation.

Known as an affiliate —or a distributor— police say the suspect operated by taking copies of the GandCrab ransomware and distributing them via email to victims across South Korea.

Between February and June 2019, the suspect sent nearly 6,500 emails to South Koreans. The emails mimicked official communications from local police stations, the Constitutional Court, and the Bank of Korea.


From 울산지방경찰청 <helpdesk@ulsanpolice.com>
Subject [울산지방경찰청]온라인 명예훼손관련 출석통지서 2019-02-11 오전 10:35
To [redacted]

울산지방경찰청
Ulsan Metropolitan Police Agency

온라인 명예훼손관련 출석통지서

귀하는 '정보통신망 이용촉진 및 정보보호 등에 관한 법률 제44조(정보통신망에서의 권리보호)' 위반으로 고소가 되어 조사를 실시할 예정임을 알려드리오니 아래의 출석요구서와 신분증 및 도장 그리고 기타 귀하가 필요하다고 생각하시는 자료를 가지고 나오시기 바라며, 이 사건과 관련하여 귀하께서 진술하고 싶은 사항 및 조사가 필요하다고 생각되는 사항이 있으시면 이를 정리한 진술서를 작성하여 출석하시기 바랍니다. 아울러 붙임과 같이 조사 시 준수할 사항을 알려드리오니 서명기재하시어 조사 시 교부하여 주시기 바랍니다.

1. 조사 목적: 온라인 명예훼손
2. 조사 기간: 2019. 02. 11 – 2019. 03. 01
3. 조사 기준일: 2019. 01. 22
4. 조사 인원: 미정
5. 조사방법: 대면 및 서면조사

붙임: 전산 및 비전산 자료 보존요청서 1부.
정보통신망 이용촉진 및 정보보호 등에 관련 법률 제 44조 위반관련 고소장 2부.
출석 요구서 1부.

2019. 03. 01까지 출석하시거나 서면제출을 하시지 않으시면
차후 불이익을 얻으실수 있습니다.

1 attachment: 출석통지서.rar 458 KB Save

However, when victims opened documents attached to emails they received, they infected themselves with the GandCrab ransomware, which then proceeded to encrypt their files and ask for a $1,300 payment in Bitcoin.

South Korean national police say they tracked at least 120 users who fell victim to the suspect's phishing campaigns.

Despite the large number of victims, authorities said the suspect only made 12 million won, which stands to around $10,500, as he only received a 7% cut from the sum victims were paying on the GandCrab ransom portal.

Suspect tracked via cryptocurrency transactions

The suspect's attacks stopped in June 2019 after the GandCrab group announced their retirement and moved on to create and run the REvil (Sodinokibi) RaaS instead, which focused on infecting companies rather than regular users.

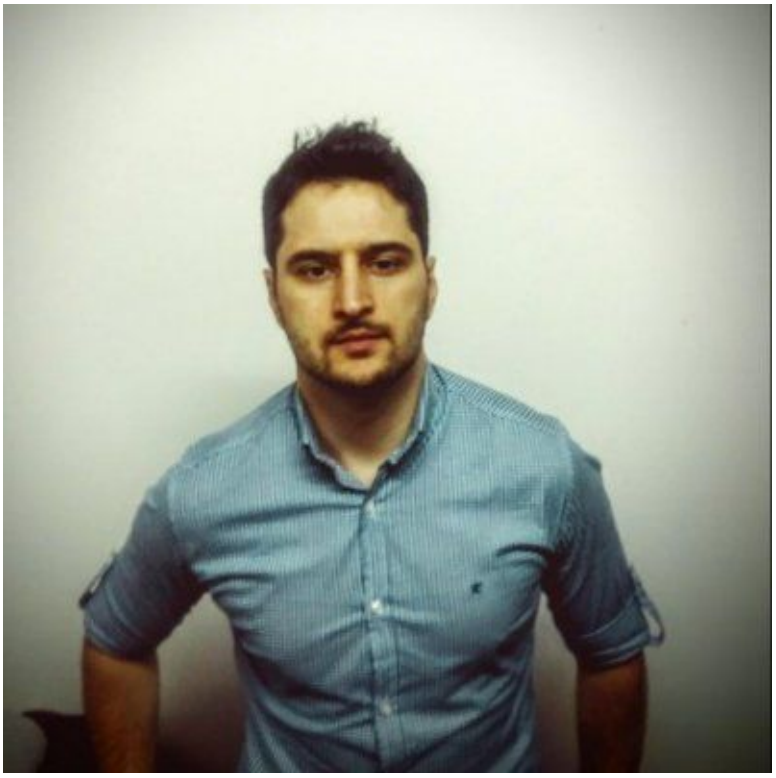
The South Korean individual marks the second GandCrab distributor arrested since the GandCrab shutdown. A 31-year-old suspect was previously arrested in Belarus in August 2020.

South Korean national police said the recent arrest, which took place last month on February 25, was the result of an international investigation led by Interpol focused on tracking down the GandCrab gang and its network of distributors. Law enforcement agencies from ten countries are involved in the investigation.

Authorities also said they tracked the suspect based on cryptocurrency transactions associated with the GandCrab operation, which led them to the suspect's bank account, despite him using a cloak of servers and IP addresses to hide his real location.

No previous article

No new articles



Catalin Cimpanu

is a cybersecurity reporter who 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.
