CISA updates Conti ransomware alert with nearly 100 domain names

By Ionut Ilascu

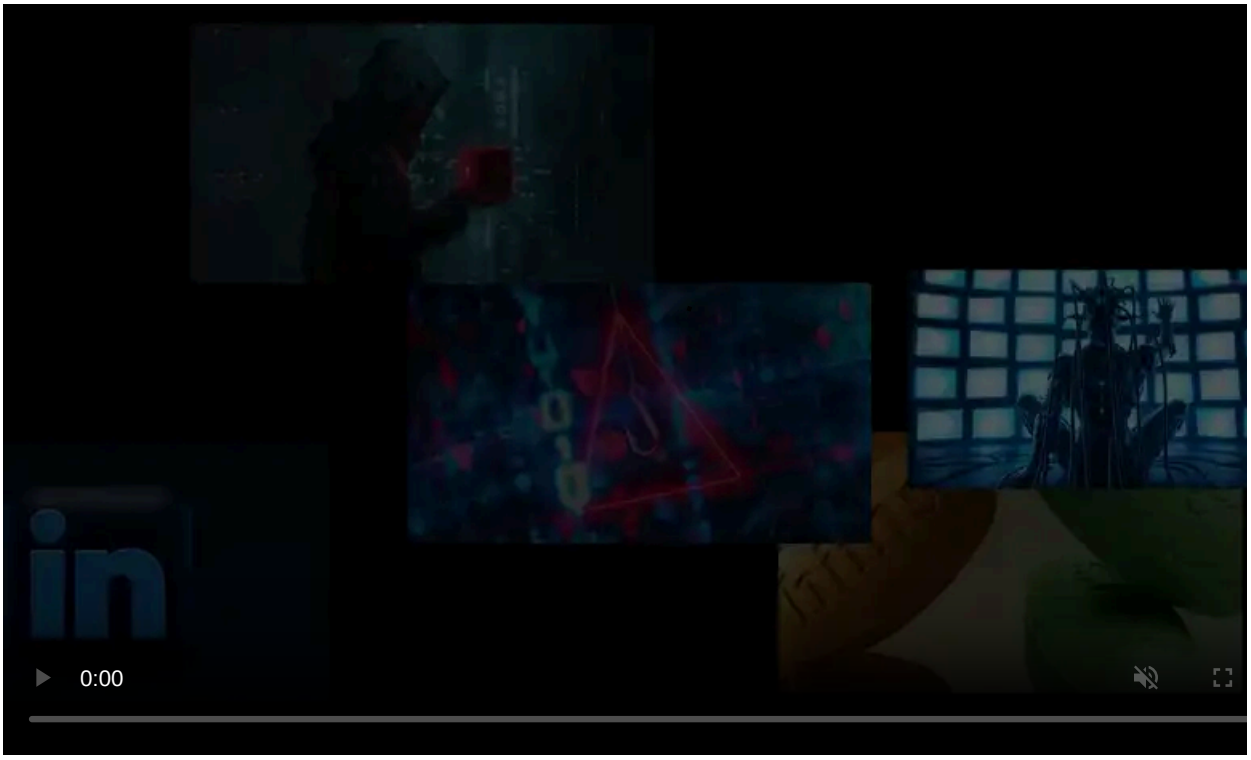
Published: 2022-03-10 · Archived: 2026-04-05 18:56:42 UTC

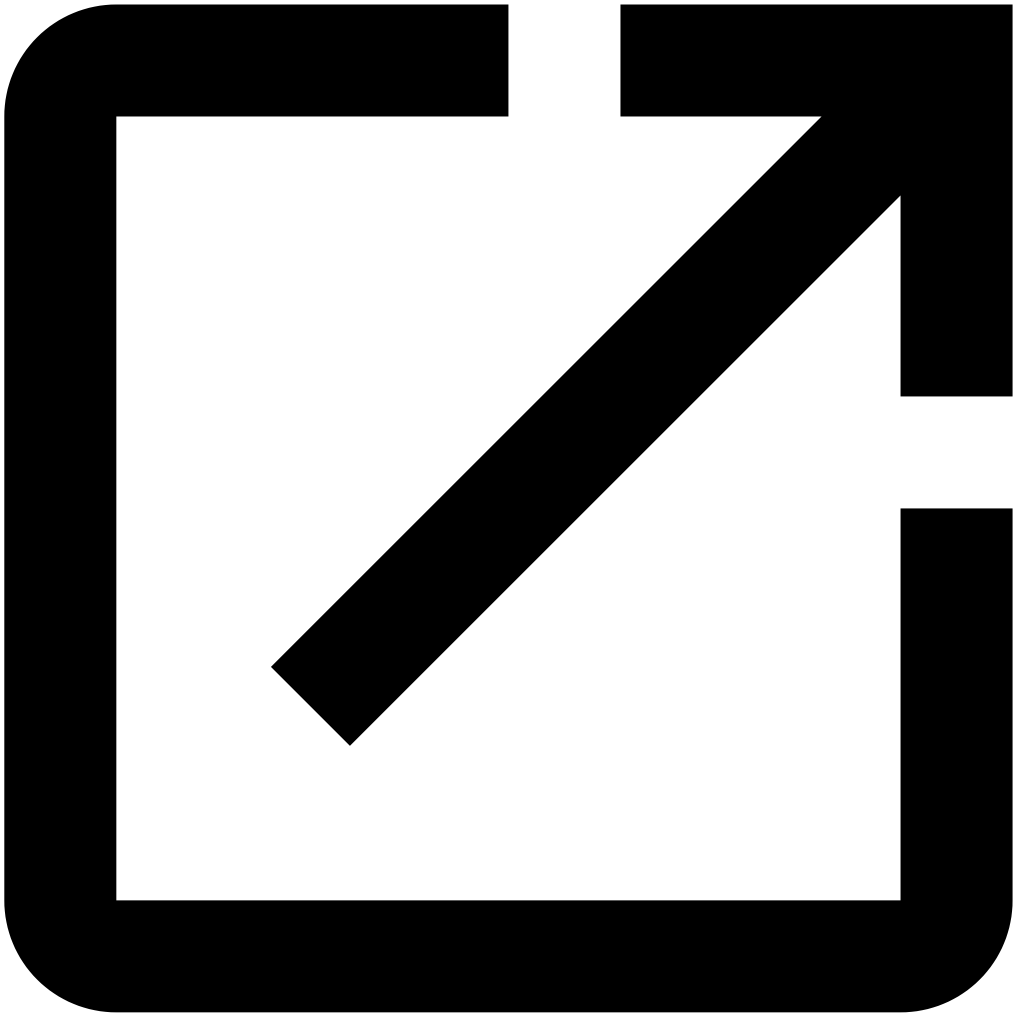
The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has updated the alert on Conti ransomware with indicators of compromise (IoCs) consisting of close to 100 domain names used in malicious operations.

Originally published on September 22, 2021, the advisory includes details observed by CISA and the Federal Bureau of Investigation (FBI) in Conti ransomware attacks targeting organizations in the U.S. The updated cybersecurity advisory contains data from the U.S. Secret Service.

Conti IoC domains

Internal details from the Conti ransomware operation started to leak at the end of February after the gang announced publicly that they side with Russia over the invasion of Ukraine.


0:00



The leak came from a Ukrainian researcher, who initially published private messages exchanged by the members of the gang and then released the source code for the ransomware, administrative panels, and other tools.

The cache of data also included domains used for compromises with BazarBackdoor, the malware used for initial access to networks of high-value targets.

CISA says that Conti threat actor has hit more than 1,000 organizations across the world, the most prevalent attack vectors being TrickBot malware and Cobalt Strike beacons.

The agency today released a batch of 98 domain names that share "registration and naming characteristics similar" to those used in Conti ransomware attacks from groups distributing the malware.

The agency notes that while the domains have been used in malicious operations some of them "may be abandoned or may share similar characteristics coincidentally."

Domains				
badiwaw[.]com balacif[.]com barovur[.]com basisem[.]com bimafu[.]com bujoke[.]com buloxo[.]com bumoyez[.]com bupula[.]com cajeti[.]com cilomum[.]com codasal[.]com comecal[.]com dawasab[.]com derotin[.]com dihata[.]com dirupun[.]com dohigu[.]com dubacaj[.]com fecotis[.]com	fipoleb[.]com fofudir[.]com fulujam[.]com ganobaz[.]com gerepa[.]com gucunug[.]com guvafe[.]com hakakor[.]com hejalij[.]com hepide[.]com hesovaw[.]com hewecas[.]com hidusi[.]com hireja[.]com hoguyum[.]com jecubat[.]com jegufe[.]com joxinu[.]com kelowuh[.]com kidukes[.]com	kipitep[.]com kirute[.]com kogasiv[.]com kozoheh[.]com kuxizi[.]com kuyeguh[.]com lipozi[.]com lujecuk[.]com masaxoc[.]com mebonux[.]com mihojip[.]com modasum[.]com moduwoj[.]com movufa[.]com nagahox[.]com nawusem[.]com nerapo[.]com newiro[.]com paxobuy[.]com pazovet[.]com	pihafi[.]com pilagop[.]com pipipub[.]com pofifa[.]com radezig[.]com raferif[.]com ragojel[.]com rexagi[.]com rimurik[.]com rinutov[.]com rusoti[.]com sazoya[.]com sidevot[.]com solobiv[.]com sufebul[.]com suhuhow[.]com sujaxa[.]com tafobi[.]com tepiwo[.]com tifiru[.]com	tiyuzub[.]com tubaho[.]com vafici[.]com vegubu[.]com vigave[.]com vipeced[.]com vizosi[.]com vojefe[.]com vonavu[.]com wezeriw[.]com wideri[.]com wudepen[.]com wuluxo[.]com wuvehus[.]com wuvici[.]com wuvidi[.]com xegogiv[.]com xekezix[.]com

The above list of domains associated with Conti ransomware attacks appear to be different from the hundreds that the Ukrainian researcher leaked from BazarBackdoor infections.

Despite the unwanted attention that Conti received recently due to the exposure of its internal chats and tools, the gang did not pull the brakes on its activity.

Since the beginning of March, Conti listed on its website more than two dozen victims in the U.S. Canada, Germany, Switzerland, U.K., Italy, Serbia, and Saudi Arabia.
