CISA updates Conti ransomware alert with nearly 100 domain names

bleepingcomputer.com/news/security/cisa-updates-conti-ransomware-alert-with-nearly-100-domain-names/

Ionut Ilascu

By
Ionut Ilascu

- March 9, 2022
- 07:31 PM
- 0

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.

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

Related Articles:

The Week in Ransomware - May 20th 2022 - Another one bites the dust

Conti ransomware shuts down operation, rebrands into smaller units

The Week in Ransomware - May 13th 2022 - A National Emergency

Costa Rica declares national emergency after Conti ransomware attacks

US offers $15 million reward for info on Conti ransomware gang

- CISA
- Conti
- Domain Name
- IoC
- Ransomware

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.

- Previous Article
- Next Article

You may also like: