The Dark Web is Getting Darker - Ransomware Thrives on Illegal Markets

bleepingcomputer.com/news/security/the-dark-web-is-getting-darker-ransomware-thrives-on-illegal-markets

The dark web is getting darker as cybercrime gangs increasingly shop their malware, phishing, and ransomware tools on illegal cybercrime markets.

In April 2022, the U.S. Treasury sanctioned the Russia-based Hydra Market. Hydra, the world's largest dark web market, provided malicious cybercrime and cryptocurrency exchange services to global threat actors. The U.S. and Germany shut Hydra down around the same time.

Ransomware groups operating on the dark web employ hundreds of hackers and earn revenues in the hundreds of millions of dollars. In addition, they could generate billions in illicit funds over time.

In 2022, researchers found 475 pages of ransomware code for sale on the dark web. Ransomware from 30 strains, including DarkSide and GoldenEye ransomware-as-a-service (RaaS), was available among these offerings.

Threat actors, including script kiddies and people with no hacking experience, increasingly join Ransomware-as-a-Service (RaaS) operations to easily get started extorting victims.

In 2022, threat actors preferred joining a RaaS for ransomware attacks as they tend to have more freedom and can deploy faster than private ransomware.

How the sale and purchase of RaaS works

Costs for joining a RaaS are low, considering the damage the malware does and the large payments it draws from victims.

For example, Venafi reported that a customized version of DarkSide, the same ransomware that criminal hackers used to close Colonial Pipeline, sold for $1,262 on the dark web.

RaaS solutions, related source code, and custom-built RaaS services sell directly on the dark web, using cryptocurrencies like bitcoin to transact the sales. For such a niche enterprise, these RaaS offerings are getting more and more legitimized—some include subscription packages, user instructions, and tech support.

Threat actors involved with these types of operations often purchase access to a network from Initial Access Brokers (IABs). Initial access includes stolen credentials that open access tools, such as Citrix, Microsoft RDP, and Pulse Secure VPN.

It's easier for criminals to buy compromised credentials than to collect the passwords themselves through phishing or brute-force attacks.

What the rise of RaaS means for cybercrime in 2023

Forecasts show Ransomware-as-a-Service operations strengthening in 2023 as they adjust operations for more efficient data exfiltration and help affiliates shame organizations that don't pay by publishing their data on leak sites.

This year, 72% of ransomware incidents used a variant that cybersecurity engineers had only seen once before.

The trend toward unique and novel ransomware attacks will continue in 2023—IABs, RaaS groups, and affiliates will increase transactions of initial access, including compromised user credentials that unlock various access tools.

The defense against rising RaaS attacks

The solution to ransomware is using a multi-layered cybersecurity defense. Defense-in-depth against ransomware attacks includes data security, endpoint security, and gateway-based security solutions.

Data Security

Data security provides backups to external, segmented networks and devices, so ransomware that encrypts production data can't get to backups.

Endpoint security

Endpoint security hardens user devices. Organizations such as NIST provide secure configurations for computers and smartphones. Endpoint security solutions combine behavior-based anti-malware and anti-phishing with ransomware protection against unauthorized changes by malicious users.

Gateway security

Gateway security safeguards users and networks against ransomware. Security gateways inspect the encrypted data that ransomware attacks use. Security gateways can detect and block ransomware from entering and leaving the network.

Locking down end-user credential entry points

Most cyberattacks use end-user credentials as network entry points. Ransomware groups buy breached credentials from IABs to gain initial access to the network in ransomware attacks.

By deploying a secure password policy organization can help users to fulfill their role in reigning in ransomware by choosing and using safe passwords.

Specops Password Policy uses Breached Password Protection, blocking over 3 billion known compromised passwords, including passwords IABs sell to ransomware groups and affiliates for initial access.

Specops Password Policy updates its breach list continually with open source as well as live-attack data from RDP honeypots.