https://www.darkreading.com/vulnerabilities---threats/threat-actors-turn-to-blockchain-infrastructure-to-host-and-hide-malicious-activity/d/d-id/1331622

Threat Actors Turn to Blockchain Infrastructure to Host & Hide Malicious Activity

4/23/2018
04:05 PM

Jai Vijayan

.bit domains are increasingly being used to hide payloads, stolen data, and command and control servers, FireEye says.

In a troubling trend for enterprises and law enforcement, threat actors are ramping up their use of blockchain domains to hide malicious activity and improve their ability to withstand takedown efforts.

Security vendor FireEye says it has observed a recent uptick in interest in cryptocurrency infrastructure in the cyber underground. Over the last year, there has been a big surge in the number of threat actors that have begun incorporating support for blockchain domains in their malware tools.

Many different software families — including some well-known ones, such as Necurs, GandCrab, Emotet, SmokLoader, and Corebot — have been reconfigured to use blockchain domains for command and control infrastructure, according to FireEye.

Searches using keywords such as Namecoin, blockchain, and .bit have also increased sharply in frequency since at least 2016, which suggests heightened criminal interest in the use of blockchain infrastructure to hide payloads, stolen data, and command and control servers.

The main advantage for threat actors in using blockchain domains is that the domains they register have no central authority — such as Internet Corporation for Assigned Names and Numbers (ICANN) or other third-party registrars — says Randi Eitzman, senior analyst at FireEye.

"In traditional ICANN-controlled domains, if a domain is known to be hosting malicious content, then law enforcement agencies could contact the central authority and request that the domain be taken down," Eitzman says.

Because blockchain top-level domains such as .bit are not centrally managed and have DNS lookup tables shared across a peer-to-peer network, takedown efforts become much more difficult. "When an individual registers a .bit — or another blockchain-based domain — they are able to do so in just a few steps online, and the process costs mere pennies."

Domain registration is not associated with an individual's name or address but with a unique encrypted hash of each user. "This essentially creates the same anonymous system as Bitcoin for Internet infrastructure, in which users are only known through their cryptographic identity."

Criminal interest in cryptocurrency-related topics are not new. As FireEye notes, threat actors have been exploring the possibility of leveraging the unique properties of blockchain technology to support malicious operations since at least 2009.

One example is malicious actors' interest in Namecoin, a Bitcoin code-based cryptocurrency that allows pretty much anyone to register and manage domain names with the .bit extension. Any individual can use Namecoin to register a .bit domain without having to directly associate their identity or address with it.

Namecoin describes itself as enabling a decentralized domain name system where domain ownership can remain completely anonymous, and domains themselves can therefore be hard to shut down without causing collateral damage.

Domains registered with Namecoin are not directly accessible via standard DNS. So, criminals increasingly have begun configuring their malware to query their own, privately managed Namecoin-compatible domain name servers in order to reach their .bit domains. Or they have been configuring the malware to query Namecoin-compatible servers that are available via underground services. In many cases, malware authors have been hard-coding blockchain-compatible DNS servers in the sample.

"Because the DNS lookup table is decentralized on a blockchain, commonly used and default DNS servers — like ones run by Google and various ISPs — are unable to resolve the domain," Eitzman explains.

Providers of so-called bulletproof hosting services have begun jumping into the fray as well. One example, according to FireEye, is Group 4, which recently has added support that allows malicious actors to query .bit-compatible servers.

FireEye expects that threat actors will continue to use Tor, domain generation algorithms, and so-called fast-flux techniques to hide malicious activity. But, increasingly, expect them to start using blockchain infrastructure as well.

"The same perks that continue to draw cybercriminals to using cryptocurrencies as a method of payment apply here," says Kimberly Goody, senior analyst at FireEye.

Blockchain domains are decentralized and more resistant to takedowns, and they provide comparative anonymity. "Due to these factors and the increasing number of malware developers supporting .bit, we can expect to see these domains to continue to grain popularity amongst threat actors," says Goody.

https://www.darkreading.com/author-bio.asp?author_id=1912

Profile of Jai Vijayan

Freelance writer

News & Commentary Posts: 519

Jai Vijayan is a seasoned technology reporter with over 20 years of experience in IT trade journalism. He was most recently a Senior Editor at Computerworld, where he covered information security and data privacy issues for the publication.

Over the course of his 20-year career at Computerworld, Jai also covered a variety of other technology topics including Big Data, Hadoop, Internet of Things, E-voting and data analytics. Prior to Computerworld, Jai covered technology issues for The Economic Times in Bangalore, India. Jai has a Master's degree in Statistics and lives in Naperville, IL.