CSO

NEWS

New IP address blacklist based on Web chatter

Traditionally, blacklists of malicious IP addresses are assembled using honeypots and intrusion detection systems but a new approach, analyzing chatter on the dark and open Web, can find malicious addresses that would have been otherwise missed

57

By Maria Korolov | Follow
CSO | Aug 11, 2015 6:00 AM PT

Traditionally, blacklists of malicious IP addresses are assembled using honeypots and intrusion detection systems but a new approach, analyzing chatter on the dark and open Web, can find malicious addresses that would have been otherwise missed.

According to Recorded Future, an analysis of 700,000 Web sources resulted in 67,563 IP addresses associated with at least one type of malware -- and 1,521 particularly dangerous IP addresses that were associated with at least two types of malware.

Of these addresses, 91 percent of the smaller list and 98 percent of the larger list were new to security researchers, and did not show up on existing blacklists, according to the report released today.

MORE ON CSO:Lost in the clouds: Your private data has been indexed by Google

One major difference between the new list and traditional lists is the higher percentage of "outbound" malicious addresses.

"An inbound address is when someone is attacking your system from an external address, trying to get in," said Staffan Truvé, chief scientist and co-founder at Recorded Future. "An outbound address is when an intruder is already in your systems, and is trying to connect to the outside world to exfiltrate data."

On traditional blacklists, 99 percent of the addresses are for inbound activity, he said.

On Recorded Future's new list, half of the addresses are for outbound activity.

For example, Recorded Future identified 476 IP addresses associated with both the Dyreza and the Upatre malware families -- only 41 of which were known to existing blacklists.

Another reason why traditional detection systems might be missing these new addresses are because the bad guys are trying to stay hidden, said Recorded Future's CEO Christopher Ahlberg.

"They'll do lots of hops along the way, so by the time they hit the honey pot, it lost the connection it originated from," he said. "But we can get back to the core of the evil."

Ahlberg stressed that Recorded Future isn't suggesting that the new list replace traditional blacklists, but can be used as a source of complementary information.

ADVERTISING

"Once you figure out that these malicious infrastructures are out there, you can block them," he said. "Or you can do more research on theme and figure out what the problem is."

For example, this kind of analysis could lead to the discovery of shared infrastructure between different malware groups.

Truvé said that Recorded Future will be integrating the new information into its threat intelligence platform.

"And the next step is integrating our system with SIEM systems, so you can automate it, have them block these addresses automatically," he said.

The company hasn't decided yet how it will share the new lists with the public.

"We publish a free daily email, the Recorded Future Cyber Daily, which today lists the top actors and top malware," he said. "So it's likely that we will be enriching that information with at least a subset of these addresses."

Maria Korolov — *Contributing Writer*

Insider: How a good CSO confronts inevitable bad news

View 2 Comments

You Might Like

.

Promoted Links by Taboola

The Ultimate Way to Get Cheap Hotel Rooms
Hotel Bargains

Build Amazing Simple Website In Only 10 Minutes !
Wix.com

How Do Pro Golfers Swing So Fast?
Revolution Golf

The Payments Industry Explained
Business Insider

The Dark Side of the App Store
Wibki.com

10 Super Cars Every Man Wants
Carophile

Taylor Swift takes on Apple, electric airplanes take off - The Wrap

Lost in the clouds: Your private data has been indexed by Google

Do boards of directors actually care about cybersecurity?

The Long And Short Of The Oil Market

TalkMarkets

Copyright © 1994 - 2015 CXO Media, Inc. a subsidiary of IDG Enterprise. All rights reserved.