Threat Brief: Understanding Domain Generation Algorithms (DGA)

By Unit 42

Published: 2019-02-07 · Archived: 2026-04-05 21:51:19 UTC

Intro

One of the most important “innovations” in malware in the past decade is what’s called a Domain Generation Algorithm (“DGA”)”. DGA is an automation technique that attackers use to make it harder for defenders to protect against attacks. While DGA has been in use for over 10 years now, it’s still a potent technique that has been a particular challenge for defenders to counter. Fortunately, there are emerging technologies now that can better counter DGAs.

What is it?

A Domain Generation Algorithm is a program that is designed to generate domain names in a particular fashion. Attackers developed DGAs so that malware can quickly generate a list of domains that it can use for the sites that give it instructions and receive information from the malware (usually referred to as “command and control” or C2).

Attackers use DGA so that they can quickly switch the domains that they’re using for the malware attacks. Attackers do this because security software and vendors act quickly to block and take down malicious domains that malware uses. Attackers developed DGA specifically to counter these actions.

In the past, attackers would maintain a static list of malicious domains; defenders could easily take that list and start blocking and taking down those sites. By using an algorithm to build the list of domains, the attackers also make it harder for defenders to know or predict what domains will be used than if they had a simple list of domains. To get that list of domains that the malware will use, defenders have to decode the algorithm which can be difficult.

Even then, taking down sites that malware using a DGA can be a challenge as defenders have to go through the process of working with ISPs to take down these malicious domains one by one. Many DGAs are built to use hundreds or even thousands of domains. And these domains are often up for only limited periods of time. In this environment blocking and taking down DGA-related domains quickly becomes a game of “whack a mole” that is sometimes futile.

Why should I care, what can it do to me?

DGA by itself can’t harm you. But it is an important piece that enables modern malware to try and evade security products and countermeasures. The importance and usefulness of DGA is best shown by the fact that it’s been in regular and constant use since at least 2008. DGA was a key component in the Conficker attacks in 2008 and 2009 and part of its success.

What can I do about it?

Because DGA is a technique the fuels malware attacks, the things you can do to help prevent malware can also help prevent DGA-fueled malware attacks:

1. Don’t open attachments that are unexpected or from unknown sources.
2. Don’t enable macros on attached documents without confirming that you can do so safely from the sender and your IT department.
3. Run security software that can help prevent malware attacks.

In addition, new technologies are being developed that can more directly counter DGA-fueled attacks, particularly for organizations. In particular, security vendors are bringing automation to bear to counter the attackers’ automation. New anti-DGA technologies that leverage machine learning and big data are capable of countering DGA’s automation with automated prediction of their own that can anticipate, block, assist with malicious site takedowns or even, in some cases, prevent those malicious sites from being used in the first place.

You can also learn more about these new technologies and look at deploying them as an additional layer of protection.

About: Threat Briefs are meant to help busy people understand real-world threats and how they can prevent them in their lives.

They’re put together by Palo Alto Networks Unit 42 threat research team and are meant for you to read and share with your family, friends, and coworkers so you can all be safer and get on with the business of your digital life.

Got a topic you want us to write about for you, your friends, or your family? Email us at u42comms@paloaltonetworks.com.
