SolarWinds/SUNBURST: DGA or DNS Tunneling?

ironnet.com/blog/a-closer-look-at-the-solarwinds/sunburst-malware-dga-or-dns-tunneling

Back to IronNet Blog
Threat Research

It's a subtle, but important, distinction for identifying attackers' behaviors — and predicting their next moves

By Peter Rydzynski, IronNet Threat Analysis Lead

Dec 21, 2020

As we continue unpacking and analyzing the SolarWinds attack, which FireEye has described as a "highly evasive" Domain Generation Algorithm (DGA) incident, we first need to agree on terminology before we can move forward with identifying and analyzing the observable behaviors.

While much of the reporting about the SUNBURST malware describes its use of DGA for command and control, we must consider whether "true" DGA behavior was at play. Could it really be DNS Tunneling? There is a subtle difference -- but this difference could have a significant impact on how we identify behaviors and start to discern the adversary's possible next steps. See, for example, previous analysis on how to detect DNS Tunneling.

DGA or DNS ? A question that's worth a deeper look.

The MITRE ATT&CK® Framework describes DGA (technique T1568.002) as follows:

"Adversaries may make use of Domain Generation Algorithms (DGAs) to dynamically identify a destination domain for command and control traffic rather than relying on a list of static IP addresses or domains. This has the advantage of making it much harder for defenders to block, track, or take over the command and control channel, as there potentially could be thousands of domains that malware can check for instructions."

ATT&CK® does not have an explicit technique assigned for DNS Tunneling; instead, it identifies this technique as a sub-technique of Command and Control Over Application Layer Protocol, described as follows:

"Adversaries may communicate using the Domain Name System (DNS) application layer protocol to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server."

To summarize the two descriptions above, DGA is the means for malicious code to identify command and control servers and avoid blocking or other defensive measures. On the other hand, DNS Tunneling is the means for malicious code to pass information to the command and control server and allow the server, in turn, to pass commands or other information back to the implanted malware.

> This distinction may seem subtle, but is critical when identifying behaviors, as well as discerning which actions the malicious actor could possibly take.

Working off the two descriptions above, we can see that the main distinction between DGA and DNS Tunneling is the structure of the queries and, most notably, the *intent* behind the queries. The effectiveness of DGA heavily relies on the structure of the queries and the hierarchical nature of the DNS protocol. Specifically, the top level domain under the registry suffix ("google" in "drive.google.com") must be dynamically generated; otherwise, identification of C2 traffic and subsequent blocking becomes relatively simple. Relating this back to the SUNBURST example, if defenders were to have put in firewall block rules to stop all queries to "*.avsvmcloud[.]com", it would effectively stop all C2 communications, thereby making this a less viable option for resilient C2. The intent behind the DNS communications observed does not appear to be identifying where a malicious C2 server is and how to reach it. Due to the ownership of the domain and control over the authoritative domain name server, the malicious code was already able to communicate with its C2 server.

SUNBURST: a case for DNS Tunneling

This second look leads us to the DNS Tunneling angle. The use case for DNS Tunneling is to enable communication between malware and C2 servers over the DNS protocol. Again, with SUNBURST, research around the structure and content of the DNS queries to "avsvmcloud[.]com" has shown that the lowest level subdomain label used for these queries is encoded data that corresponds to the active directory domain name of the infected network. This does not lend itself to the DGA use case, as the top domain under the registry suffix is not changing and makes blocking such traffic at the firewall trivial. This does, however, provide the threat actor with accurate information about which network — and possibly even which infected host — was making the query, a critical function when managing a vast number of infections across a broad set of environments. Furthermore, the

responses to these queries are not indicative of the actual IP addresses for C2 servers. Rather, they indicate the command or action that the threat actor wants the malicious implants to take. This is exactly the way DNS Tunneling functions.

IronNet's DNS Tunneling analytic

IronNet's DNS Tunneling analytic detects the use of DNS traffic as a covert network channel. Data can be hidden in DNS messages using encoded subdomain labels and resource records, and then transferred through the normal domain name resolution process. DNS Tunneling may indicate the presence of adversary communications with implanted malware or covert transmission of sensitive information from the enterprise. There are a number of malicious tools that have leveraged this technique, including Pisloader and ALMA Communicator, as well as point-of-sale malware, such as Multigrain/NewPosThings, which have used DNS Tunneling to transfer credential and credit card information.

In the case of SUNBURST, the malware utilized DNS Tunneling to relay information about the infected network. Researchers have determined that the encoded subdomain labels at a minimum transmit the domain name of the infected host (which IronNet has validated) and likely pass additional information about the infected system. The resolved IP addresses, transmitted in the returned A record response, are in turn used to provide instructions back to the malware.

Moving forward post-SUNBURST

The gravity of the SolarWinds/SUNBURST attack is yet to be determined. In the meantime, we will continue to share our analysis, including updates by my colleague Adam Hlavek on the Russian cyber attack threat landscape at large, for the greater good of collective, widespread, and fast recovery of this rampant attack.

Back to IronNet Blog