SolarWinds: How a Rare DGA Helped Attacker Communications Fly Under the Radar

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-unique-dga

Threat Hunter TeamSymantec

In the second of a series of follow-up analysis on the SolarWinds attacks, we examine how the attackers made command and control communications particularly stealthy.

In the weeks since news of the SolarWinds attacks broke, we've continued our analysis into the tools used by the attackers. One of the most interesting things we've seen is the way the attackers configured their malware in order to contact a command and control (C&C) server via DNS communications. It's a technique that is rarely used, but there have been some reports of other APT groups such as Crambus (aka Oilrig) using it previously.

Sunburst (Backdoor.Sunburst), the malware which was used to Trojanize the SolarWinds Orion software, uses a domain generation algorithm (DGA) to generate domain names to contact for C&C purposes. However, unlike most DGAs, this DGA does not just randomly generate characters. Instead, information is encoded into the text that makes up the generated domain names. By doing so, initial C&C actually happens via DNS, which provides a stealthier level of communications.

For each infected computer, Sunburst generates a unique ID, referred to as a userid. The userid is made up of the first active MAC address that is not the loopback address, concatenated with the Windows Domain name of the computer, and then concatenated with the Windows installation UUID, a randomly generated value at Windows installation time stored in HKLM\SOFTWARE\Microsoft\Cryptography\MachineGuid. These three values are then MD5 hashed and the first 64 bits are XOR'd with the last 64 bits, resulting in a unique 64-bit userid.

Because multiple DNS requests will have to be made to transmit all payload information, the attackers require a unique ID to know from which computer the information is coming from. DNS is a distributed protocol, meaning the infected computer does not contact the attacker's C&C server directly, but instead the DNS request is passed through multiple intermediaries before reaching the attacker DNS server. Only by including the userid within the DNS request will the attackers be able to combine the multiple requests.

The DNS lookup will be in one of the following forms:

<encoded information>.appsync-api.eu-west-1.avsvmcloud.com

<encoded information>.appsync-api.us-west-2.avsvmcloud.com

<encoded information>.appsync-api.us-east-1.avsvmcloud.com

<encoded information>.appsync-api.us-east-2.avsvmcloud.com

The encoded information will be in one of two forms providing the attackers either the Windows domain name of the infected organization or security product statuses and feedback on the infected machine.

Windows Domain Name Payload

Initially, after Sunburst checks for or bypasses security tools and products, the first DNS lookup will occur containing the infected computer's Windows domain name or a portion thereof, encoded into the C&C domain. The Windows domain is usually a human-readable string representing the name of the organization the machine belongs to, e.g. AcmeA1Corp.

The DGA will start by prepending the aforementioned userid with a randomly chosen key byte between 0x81 and 0xFE followed by the userid XOR'd with the key byte. These nine bytes are then encoded in a fashion similar to Base64, resulting in 15 characters.

This string of characters is then followed by the Windows domain name, encoded. Because Windows domain names can be up to 253 characters long, Sunburst chooses to segment the Windows domain names into 14 character chunks preceded by the chunk number (where the first chunk number is 0). Windows domain names longer than 14 characters will thus require more than one DNS lookup to provide the entire Windows domain name.

Sunburst will also resend previously sent chunks if an error was encountered or, under certain error conditions, set the chunk number to a negative one. The segment chunk number and the Windows domain name are both encoded separately and appended to the encoded userid. These elements form the subdomain of the domain. This domain is queried via DNS, which results in this encoded information reaching the attacker's DNS server. The attacker can then decode the information and reply with further instructions, which will be covered in a future blog.

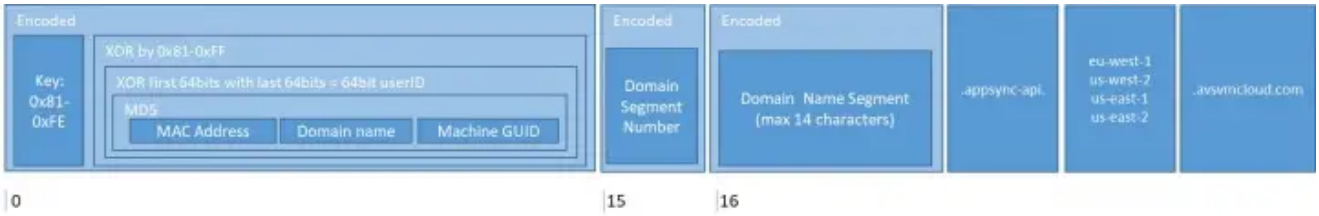

Figure 1. Structure of Sunburst DNS lookups

Sunburst does not automatically generate multiple DNS queries in order to send the entire Windows domain name. Whether Sunburst will send the remaining 14-character segments depends on the response received from the initial DNS query. Because Sunburst was delivered via a supply chain attack, many systems that are not of interest will be infected. By encoding the first 14 characters of the Windows domain name into the first DNS query, the

attackers are able to triage infections and only mount second-state attacks on systems of interest - those that have Windows domain names that match organizations they wish to target.

Security Product Status and Feedback Payload

Depending on the response to the first DNS lookup, a second DNS lookup may occur that encodes the status of installed security products on the system and information on whether the DNS communication has been successful.

First, the userid is XOR'd by the third and second bytes of a timestamp value described below in an alternating fashion before being XOR'd by a randomly chosen key byte between 0x01 and 0x7E that is then prepended to the userid. The first byte thus provides not only the key byte, but informs the attackers if the remaining content will contain the Windows domain name payload (key byte is between 0x81 and 0xFE) or the security product status and feedback payload (key byte is between 0x01 and 0x7E).

After the userid, a nibble (half a byte) is used to specify if the security payload information has content (nibble is set to 2) or is blank (nibble is set to 1). This is followed by a timestamp in UTC of when the DNS query was sent, granular to 30-minute increments. The last bit of the timestamp is set to a bit flag representing whether the previous DNS response successfully contained partial or full instructions to start the secondary HTTP communication channel. This may have been designed by the attackers as a feedback mechanism to ensure the DNS communication mechanism is working before sending the full HTTP communication channel details and, in the case of full details, a signal that the HTTP communication should have already started. After the timestamp, the security product status payload is optionally provided if select security product services were found as running.

The two bytes contain a bitmask that encodes information on whether any of the following security products were not found, or found running and/or subsequently disabled and stopped:

- CrowdStrike
- Carbon Black
- FireEye
- ESET
- F-Secure
- Microsoft Defender

The userid, timestamp, feedback bit, and optional security product data are then encoded into text as the subdomain of a DNS query that is sent to the attackers.

Figure 2. Structure of second DNS lookup communicating security product status

The responses to these DNS queries may then contain control information for the threat to terminate or launch a secondary HTTP communication channel, something that we plan to cover in a subsequent blog.

Protection/Mitigation

Tools associated with these attacks will be detected and blocked on machines running Symantec Endpoint products.

File-based protection:

- Backdoor.Sunburst
- Backdoor.Sunburst!gen1
- Backdoor.SuperNova
- Backdoor.Teardrop

Network-based protection:

System Infected: Sunburst Malware Activity

About the Author

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.

Want to comment on this post?