

# SUNBURST: Backdoor em cadeia de abastecimento compromete sistemas americanos

Empresas gigantes de tecnologia e segurança da informação foram comprometidas



No começo de 2021, veículos midiáticos ao redor do mundo foram tomados por notícias de um ataque que supostamente havia comprometido sistemas essenciais do governo americano, com APTs patrocinadas pela inteligência russa no centro de algumas das acusações. O ataque é considerado uma das piores ocorrências de espionagem já sofridas pelo governo americano, tanto pelo perfil dos alvos afetados (que incluiu entidades desde a Microsoft até a OTAN) quanto pela duração do ataque, que durou meses até ser descoberto.

## Descrição

No final de 2020, uma reportagem do *The New York Times* descrevia um ataque - provavelmente de autoria russa - sobre a empresa de segurança da informação americana FireEye. A empresa em questão é tida como uma das gigantes do ramo nos Estados Unidos e no mundo, atuando na detecção e prevenção de ataques cibernéticos, com alguns de seus serviços incluindo testes de invasão para empresas indexadas pelo S&P 500 e monitorando grupos considerados *Advanced Persistent Threats* (APTs) para órgãos públicos, entre eles a própria agência de segurança nacional americana, a NSA.

Segundo a empresa americana, o ataque havia obtido sucesso em roubar algumas de suas ferramentas de *red teaming* - Armas digitais usadas para testes de invasão, armazenadas em cofres digitais da companhia de cibersegurança e que poderiam representar ameaças sérias nas mãos de adversários. Como parte do esforço de mitigação, a FireEye disponibilizou regras de YARA em seu GitHub como contramedidas que permitem a detecção das ferramentas de ataque vazadas. Mas o pior ainda estava por vir - durante a investigação do ataque, profissionais da empresa descobriram um problema muito maior.

No meio de 50.000 linhas de código que estavam sendo investigadas por possíveis comprometimentos, integrantes da Mandiant (equipe de resposta de incidentes da FireEye) descobriram uma vulnerabilidade dentro do software de monitoramento de redes Orion produzido pela SolarWinds Corp, que abrigava um backdoor dentro dos sistemas da empresa. A escala do problema era inimaginável: O software em questão era digitalmente assinado pela empresa do Texas, e portanto havia sido enviado para todos os seus clientes num processo conhecido como *supply chain attack* - Entre os afetados estavam empresas como a Cisco, Malwarebytes, NVIDIA, Microsoft, e departamentos e agências como a NSA, o FBI, o Departamento de Estado e Departamento de Defesa dos Estados Unidos.

Em seu relatório, a empresa americana chamou a vulnerabilidade encontrada de SUNBURST, e a Microsoft posteriormente adicionou regras de detecção ao Windows Defender. Em um cenário de crescentes tensões no aspecto de segurança da informação envolvendo os EUA, a Rússia, China e o Irã, o ataque (ou a descoberta dele) foi considerado um dos primeiros desafios de relações exteriores a ser enfrentado pelo recém inaugurado presidente dos EUA, Joe Biden.

# SUNBURST

## Anti-Threat Analysis

O nível de sofisticação do ataque foi alto - Os hackers conseguiram comprometer o servidor responsável por armazenar e distribuir os updates para o software Orion da SolarWinds, o que resultou na distribuição eficiente dos trojans. E como esses updates eram digitalmente assinados pela SolarWinds, a chance de detecção do malware era mínima. De fato, é possível que se não fosse pelo ataque à FireEye que resultou na investigação de seus softwares, o comprometimento dos servidores passaria despercebido até hoje.

Assim como a maioria dos malwares modernos (mas fazendo uso de uma sofisticação substancialmente maior), o SUNBURST possui vários mecanismos de anti-análise que, segundo a FireEye, foram o que o permitiu evitar detecção por softwares de anti-vírus e forenses profissionais por sete meses. Tais mecanismos se caracterizam pela realização de checagens que testam o sistema por alguns requisitos básicos que garantem para o vírus que este esteja operando em um computador real e não em uma máquina virtual usada para análise forense de softwares maliciosos, por exemplo. Em malwares mais simples, se verificam a presença de certa quantidade (em gigabytes ou terabytes) de memória RAM e de HD, conexão com a internet, entre outros.

As checagens do SUNBURST antes de sua execução eram substancialmente mais complexas. Por exemplo, o malware verificava se o nome do processo contendo o código malicioso era `solarwinds.businesslayerhost` conforme o esperado - Mas o nome do processo dentro do malware era hashado e usava-se uma função XOR para compará-lo com o nome dentro da máquina infectada e assim dificultar a verificação. Após a verificação do nome do processo, o SUNBURST ficava quieto por cerca de duas semanas antes de verificar se a última escrita na biblioteca `SolarWinds.Orion.Core.BusinessLayer.dll` também havia se dado cerca de duas semanas depois da execução inicial do malware, e na sequência criava uma **named pipe** para seu uso próprio. Na sequência, o SUNBURST armazena suas configurações em um arquivo chamado `SolarWinds.Orion.Core.BusinessLayer.dll.config` modificado para permitir controle do malware a partir de centros de Comando e Controle (C2), e faz verificações referentes ao serviço de **Active Directory** - Se o sistema não está em um domínio contendo esse serviço, ou se está em um dos domínios que contém AD mas que está na blacklist de domínios indesejados do malware, este encerra suas atividades.

Por último, o trojan verifica a conectividade com a Internet, tentando resolver o DNS do domínio `api.solarwinds.com`

## Infraestrutura de Comando e Controle

Após as checagens de anti-análise, o SUNBURST cria um servidor de comando e controle intermediário, com o fim de definir o modo de operação a ser utilizado e enviar informações a respeito do servidor C2 final, controlado pelo atacante. Para impedir a detecção, o malware faz

uso de um **algoritmo de geração de domínios (DGA)** que faz uso de informações da vítima para criar nomes de domínios que pareçam legítimos. Os nomes de domínios gerados então eram sufixados com domínio do servidor C2 intermediário referente ao modo de operação desejado, como por exemplo:

- `<nome-do-domínio-gerado>. appsync-api. eu-west-1[.]avsvmcloud[.]com`
- `<nome-do-domínio-gerado>. appsync-api. us-east-2[.]avsvmcloud[.]com`

Posteriormente, a comunidade fez engenharia reversa no algoritmo DGA descoberto e disponibilizou scripts para decodificação de nomes de domínio.

Durante a utilização do backdoor, o tráfego de comunicações se dá de formas tanto ativas quanto passivas. O modo ativo usa o protocolo HTTP para receber comandos por meio do servidor C2 e o modo passivo usa o protocolo DNS para fazer *beaconing* para receber atualizações de status. Por exemplo, respostas de DNS do tipo A (*DNS A responses*) dentro de alguns ranges de IP instruem o SUNBURST a continuar fazendo *beaconing*:

```
8. 18. 144. 0/23
18. 130. 0. 0/16
71. 152. 53. 0/24
99. 79. 0. 0/16
87. 238. 80. 0/21
199. 201. 117. 0/24
184. 72. 0. 0/15
```

Enquanto *DNS A responses* nessas outras ranges de IP instruem o malware à encerrar suas atividades, atualizando o valor do parâmetro `ReportWatcherRetry` dentro do arquivo de configuração `SolarWinds.Orion.Core.BusinessLayer.dll.config`.

```
10. 0. 0. 0/8
172. 16. 0. 0/12
192. 168. 0. 0/16
224. 0. 0. 0/3
fc00:: - fe00::
fec0:: - ffc0::
ff00:: - ff00::
20. 140. 0. 0/15
96. 31. 172. 0/24
131. 228. 12. 0/22
144. 86. 226. 0/24
```

No caso de uma resposta CNAME vinda do servidor DNS no C2 intermediário, o SUNBURST vai usar o protocolo HTTPS para abrir uma comunicação para o servidor C2 final a partir do domínio

especificado na resposta. Uma lista completa dos comandos que podem ser enviados ao SUNBURST e suas operações correspondentes pode ser encontrada no artigo de Alexis Rodriguez no Medium. Observando o modo de operação descrito no parâmetro `ReportWatcherRetry`, integrantes de *Blue Teams* respondendo à incidentes de segurança envolvendo o backdoor da SUNBURST podem inferir as últimas operações realizadas pelo malware antes do fim de suas operações, onde:

- 3 - (Truncate) O interruptor do malware foi ativado e suas operações foram encerradas por definitivo a não ser que modificações externas sejam aplicadas;
- 4 - (New) Modo passivo - O algoritmo DGA gera subdomínios que obfusca o nome de domínio do sistema e do servidor C2 intermediário;
- 5 - (Append) Modo ativo - O beaconing do servidor de comando e controle está para ocorrer assim que um DNS CNAME seja resolvido ou já está ocorrendo.

## Algumas ferramentas de contramedidas:

- Mandiant Azure AD Investigador - Detecta indícios de atividade do SUNBURST
- FireEye Red Team Tool Contermeasures - Regras de YARA, Snort, ClamAV e HXIOC para detectar assinaturas das Red Team Tools vazadas da FireEye
- FireEye Mandiant SUNBURST Contermeasures - Regras de YARA, Snort, ClamAV e HXIOC para detectar assinaturas do SUNBURST

## Conclusão

Os ataques à SolarWinds figuram entre alguns dos maiores ataques cibernéticos entre atores estatais já registrados, e suas consequências diplomáticas refletem o que foi registrado. Durante as sanções anunciadas pela Casa Branca sobre a Rússia no dia 15/04, seis empresas e institutos de pesquisa nas áreas de TI e Segurança da Informação russos foram incluídos após Washington formalmente culpar a inteligência russa pelo ocorrido.

O aumento exponencial de casos no que se refere à ataques cibernéticos por meio desses grupos (que atuam como *proxies* de atores estatais) representa uma mudança cada vez mais comum no que diz respeito a táticas de Inteligência, de guerra não-convencional e na geopolítica como um todo, e nações que não se comprometerem com investimentos em inovações também nas áreas de informática e segurança da informação estarão cada vez mais vulneráveis.

Para ler mais, visite os links (também usados de fonte para esta página):

- Palestra dada na FireEye Virtual Summit onde a atuação do SUNBURST é explorada
- <https://medium.com/swlh/a-summary-of-fireeyes-detailed-analysis-on-the-sunburst-malware-d76cef328a3b>
- <https://0xthreatintel.medium.com/internals-of-sunburst-malware-93c4cac46db6>
- <https://www.fortinet.com/blog/threat-research/what-we-have-learned-so-far-about-the->

sunburst-solarwinds-hack

- <https://www.fireeye.com/current-threats/sunburst-malware.html>
  - <https://www.fireeye.com/blog/threat-research/2020/12/sunburst-additional-technical-details.html>
  - <https://www.brighttalk.com/webcast/7451/469525>
  - <https://www.varonis.com/blog/solarwinds-sunburst-backdoor-inside-the-stealthy-apt-campaign/>
  - <https://www.npr.org/2020/12/21/948843356/how-a-cybersecurity-firm-uncovered-the-massive-computer-hack>
- 

Revision #12

Created Mon, Apr 5, 2021 11:09 PM by Victor

Updated Fri, May 14, 2021 12:44 PM by Victor