FORTRESS
Information Security

Threat Intelligence Report

DOE Subcontractor Sol Oriens Experiences Data Breach

June 15, 2021

Date: June 15, 2021
https://www.fortressinfosec.com

Fortress Information Security, LLC
Phone: 855.FORTRESS
189 S. Orange Ave., Orlando, FL 32801

Table of Contents

**The usage and distribution of this document is strictly governed by the terms of our agreement with our client, and this document may not be relied upon anyone other than our client. Only individuals with a specific contractual right to view this document may do so, and if you believe you may have received this document in error, please do not read further and contact us via email at Compliance@FortressInfoSec.com as soon as possible.

To the extent this document is provided to or obtained by a governmental entity, please note that confidential treatment of this document is requested under both the Freedom of Information Act, as well as any similar applicable state or local laws governing the public disclosure of documentation, and written notice of any request for this document is requested to be sent to us via email at Compliance@FortressInfoSec.com as soon as possible.

The analysis set forth herein is made as of the date listed in this document, and we are under no obligation to correct or modify this document on an ongoing basis, unless we have specifically contracted with our client to do so in a mutually executed agreement. The usage of critical, high, medium, moderate, nominal, low, or other scaled indicators or parlance associated with the rating of risk is based on our subjective determinations, and our subjective determinations may deviate from regulatory determination, and determinations by others. Our determinations are based on facts and data we receive, and to the extent any facts or data are incorrect, our determinations may then be correspondingly incorrect. Any included recommendations provided are non-inclusive and are only intended to serve as exemplar actions to address security risks, rather than as the sum-total of all actions recommended to address security risks.

Information security threats change on a daily basis, and no amount of security testing or verification can ensure that any systems or hardware are fully secure from unauthorized access. We make no guarantees or representations of accuracy beyond those contained in any mutually executed agreement with our client that address the contents of this document. This document only provides our findings under the terms of our agreement with our client and does not constitute a representation or warranty that any systems or hardware are advisable to use or free of defects or malicious code.

Executive Summary

In May 2021, Sol Oriens, a subcontractor for the Department of Energy (DOE) who works with the National Nuclear Security Administration (NNSA), was the subject of a cyberattack which originated from the known ransomware group REvil. Specific details surrounding how the attack was executed, including the initial intrusion vector, are unknown at this time. The attackers were able to steal employee names, social security numbers, pay rates, a contracts ledger, and information related to employee training programs, all of which were posted on the dark web. While more sensitive information does not appear to have been exfiltrated, this incident highlights the threat posed by breaches affecting critical suppliers of US government entities.

Fortress Information Security (FIS) will continue to monitor this threat and will update this report as new information is observed.

Threat Identification

In May 2021, Sol Oriens was the subject of a cyberattack which originated from the REvil ransomware group. The attackers were able to steal employee names, social security numbers, pay rates, a contracts ledger, and information related to employee training programs, all of which were posted on REvil’s dark web blog. There is no publicly disclosed evidence at present that suggests any highly-confidential information was stolen; however, the possibility remains that REvil stole additional data and chose not to publicly release it, either to use for further extortion of Sol Oriens or to sell to the highest bidder. In addition, the information stolen in this attack may be leveraged by threat actors to enable future sophisticated phishing attacks targeting Sol Oriens employees, heightening the risk the company will be compromised again in the future.

In-Depth Threat Analysis

REvil

REvil (also known as Sodinokibi/Sodin) has been active since at least 2019. The REvil Ransomware-as-a-Service (RaaS) shares similarities to the GandCrab RaaS which was linked to the Gold Southfield Group, suggesting the attackers responsible for the malware have been active for even longer. REvil is believed to be based in Russia, as the threat actor group does not target organizations within Russia or other former Soviet territories.

REvil first made headlines in 2019 after a successful ransomware attack on Travelex, who reportedly paid a 2.3 million dollar ransom. Since then, REvil has become notorious for targeting large organizations, and demanding massive ransom payments. In 2021 alone, REvil has targeted the following organizations:

- **April 2021 – Quanta Computer and Apple** – REvil compromised Quanta Computer, a primary supplier for Apple, and attempted to extort a 50 million dollar ransom in exchange for not releasing information related to upcoming Apple products. After Quanta was unwilling to comply, REvil then shifted their focus and demanded that Apple pay the ransom.

- **May 2021 – JBS Foods** – REvil successfully compromised JBS Foods and temporarily shut down the company's operations in both the United States and Australia. JBS eventually paid the demanded ransom of 11 million dollars, reportedly in an effort to protect their customers and employees. After this attack, a member of REvil said in an interview that their original was not JBS, but was instead an unnamed Brazilian organization.

MITRE ATT&CK Analysis

The MITRE ATT&CK framework is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target. Below is a list of various phases and attack types used by REvil.

T1134	Access Token Manipulation: Token Impersonation/Theft	REvil can obtain the token from the user that launched the explorer.exe process to avoid affecting the desktop of the SYSTEM user.
T1134	Access Token Manipulation: Create Process with Token	REvil can launch an instance of itself with administrative rights using runas.
T1071	Application Layer Protocol: Web Protocols	REvil has used HTTP and HTTPS in communication with C2.
T1059	Command and Scripting Interpreter: Visual Basic	REvil has used obfuscated VBA macros for execution.
T1059	Command and Scripting Interpreter: Windows Command Shell	REvil can use the Windows command line to delete volume shadow copies and disable recovery.
T1059	Command and Scripting Interpreter: PowerShell	REvil has used PowerShell to delete volume shadow copies and download files.
T1485	Data Destruction	REvil has the capability to destroy files and folders.
T1486	Data Encrypted for Impact	REvil can encrypt files on victim systems and demands a ransom to decrypt the files.
T1140	Deobfuscate/Decode Files or Information	REvil can decode encrypted strings to enable execution of commands and payloads.
T1189	Drive-by Compromise	REvil has infected victim machines through compromised websites and exploit kits.
T1573	Encrypted Channel: Asymmetric Cryptography	REvil has encrypted C2 communications with the ECIES algorithm.
T1041	Exfiltration Over C2 Channel	REvil can exfiltrate host and malware information to C2 servers.
T1083	File and Directory Discovery	REvil has the ability to identify specific files and directories that are not to be encrypted.
T1562	Impair Defenses: Disable or Modify Tools	REvil can connect to and disable the Symantec server on the victim's network.
T1070	Indicator Removal on Host: File Deletion	REvil can mark its binary code for deletion after reboot.
T1105	Ingress Tool Transfer	REvil can download a copy of itself from an attacker-controlled IP address to the victim machine.

T1490	Inhibit System Recovery	REvil can use vssadmin to delete volume shadow copies and bcdedit to disable recovery features.
T1036	Masquerading: Match Legitimate Name or Location	REvil can mimic the names of known executables.
T1112	Modify Registry	REvil can save encryption parameters and system information to the Registry.
T1106	Native API	REvil can use Native API for execution and to retrieve active services.
T1027	Obfuscated Files or Information	REvil has used encrypted strings and configuration files.
T1069	Permission Groups Discovery: Domain Groups	REvil can identify the domain membership of a compromised host.
T1566	Phishing: Spearphishing Attachment	REvil has been distributed via malicious e-mail attachments including MS Word Documents.
T1055	Process Injection	REvil can inject itself into running processes on a compromised host.
T1012	Query Registry	REvil can query the Registry to get random file extensions to append to encrypted files.
T1489	Service Stop	REvil has the capability to stop services and kill processes.
T1082	System Information Discovery	REvil can identify the username, machine name, system language, keyboard layout, OS version, and system drive information on a compromised host.
T1007	System Service Discovery	REvil can enumerate active services.
T1204	User Execution: Malicious File	REvil has been executed via malicious MS Word e-mail attachments.
T1047	Windows Management Instrumentation	REvil can use WMI to monitor for and kill specific processes listed in its configuration file.

Impact

Based on the broad range of industries targeted by REvil in 2021 alone, it is unlikely that the attackers intentionally targeted Sol Oriens with the intent of affecting US government operations. Instead, Sol Oriens was most likely simply a target of opportunity. Regardless of intent, the attack had the potential to both disrupt the operations of and compromise sensitive data belonging to the US Department of Energy and the National Nuclear Security Administration. The information stolen in this attack may be leveraged by threat actors to enable future sophisticated phishing attacks targeting Sol Oriens employees, heightening the risk the company will be compromised again in the future.

Security Recommendations and Mitigation Strategies

Mitigation

To mitigate these types of attacks, organizations should ensure patches are up to date, consider implementing two factor authentication for both external and internal components, and disabling any outward facing ports that may not necessary, including RDP, which is commonly used by attackers to compromise networks. After the necessary hardening of systems has been completed, employees should be continuously trained to recognize social engineering techniques such as phishing emails.

Fortress Information Security Recommendations

Fortress Information Security (FIS) recommends companies take defensive measures to minimize the risk of exploitation of vulnerabilities. Specifically, companies should:

Implement Controls to Prevent and Detect Malware Deployment:

- Ensure that antivirus/endpoint protection software is deployed on all endpoints. Antivirus signatures should be kept updated to ensure it is protecting against the latest threats.
- Monitor outbound network traffic for any suspicious activity – this could serve as an indicator of malware attempting to communicate with a Command and Control (C2) server.
- Ensure your security tools are monitoring for known indicators of compromise.
- Malware is frequently delivered by phishing emails, so ensure that users are trained not to open attachments or click on links from suspicious sources.

Protect your Network from External Attackers:

- Ensure all network and system resources are properly protected by firewalls, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS).
- Configure firewalls to block known malicious IP addresses.
- If remote access to corporate resources is needed, be sure employees use a Virtual Private Network (VPN).
- Ensure that your company maintains an up-to-date inventory of all externally facing assets. Maintaining an accurate asset inventory is critical in ensuring defensive measures are properly deployed across the entire perimeter.

Implement a Strong Phishing Defense Program:

- Ensure end users are properly trained to detect and respond to phishing attacks. Employees should know not to open attachments or click links from suspicious sources, and how to report phishing emails.
- Consider implementing a live phish training program, which allows users to practice responding to phishing attacks and helps identify employees who need additional training.
- Scan all incoming emails to detect threats and filter executable files from reaching end users.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email to prevent email spoofing.

Develop a Data Loss Prevention Program:

- Ensure system monitoring is in place to be able to track who is accessing specific files. This will help pinpoint exactly when files were extracted and who was involved.
- Scan all outgoing emails to detect any potential confidential data leaving the company’s network.
- Consider limiting access to cloud storage websites that can be accessed from outside of the corporate network. If there is not a legitimate business need to use these types of websites, they may present undue risk of data exfiltration.
- Limit users’ ability to store data on external storage devices, unless there is a business need to do so.

Have a Vendor Risk Management Program:

- Security breaches at vendors that have access to your company’s data or systems can pose just as much of a threat as a data breach at your company. Ensure you have a program in place to manage these risks and respond to vendor breaches when they occur.
- Ensure that network traffic and email communications between your company and its vendors is monitored for any anomalies that could indicate malicious activity.
- Evaluate all vendors’ security controls regularly to ensure they align with your company’s risk posture.

FIS reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.