

M365 Defender

Corina Feuerstein

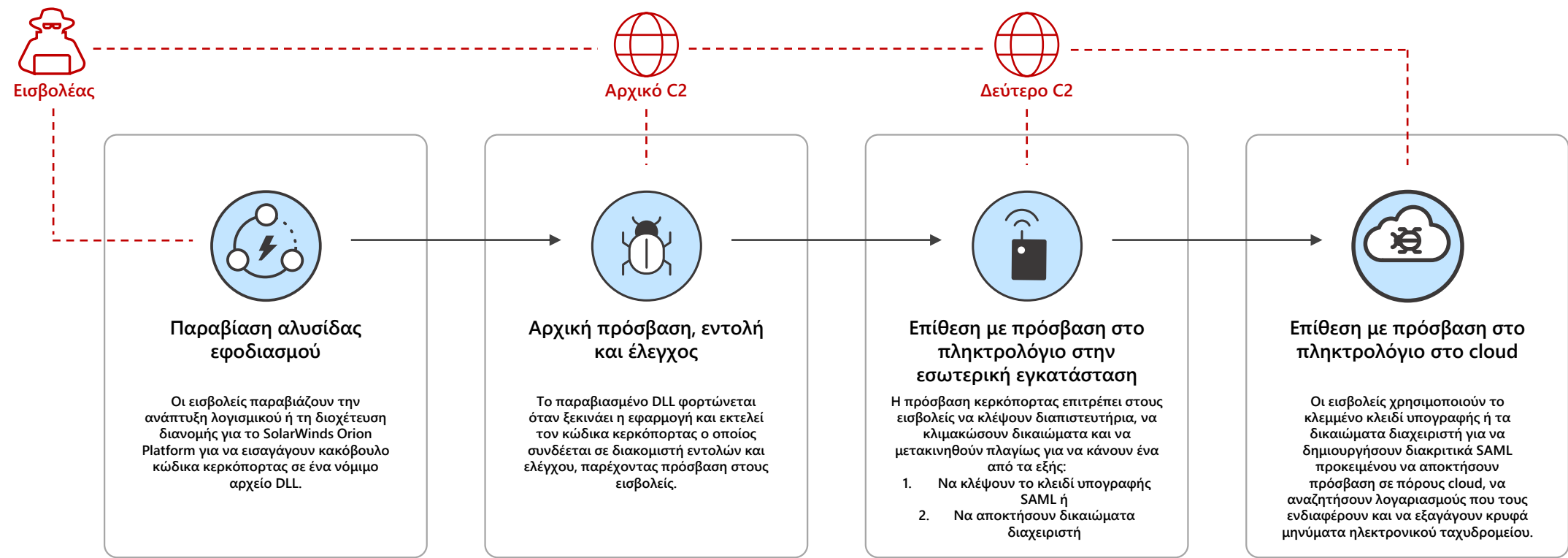
Υπεύθυνη διαχείρισης προγράμματος
M365 Defender

18 Φεβρουαρίου 2021

Χρήση του Microsoft 365 Defender για εντοπισμό, προστασία και αποκατάσταση

1. Πώς συνέβη η επίθεση Solorigate
2. Εντοπισμός και αποκλεισμός δραστηριότητας τελικού σημείου εσωτερικής εγκατάστασης
3. Εντοπισμός παραβίασης ταυτότητας και συγκεντρωτική προβολή στο cloud
4. Εντοπισμός και απάντηση σε ύποπτη δραστηριότητα εφαρμογής cloud
5. Κατανόηση της έκθεσης του οργανισμού και των αμβλύσεων με χρήση της Ανάλυσης απειλών
6. Εντοπισμός μεταξύ τομέων με το Microsoft 365 Defender

Επισκόπηση Solorigate



Κακόβουλη επικοινωνία C2 που έχει αποκλειστεί από MDE

Network traffic to domains associated with a supply chain attack

Part of incident: Multi-stage incident involving Execution & Command and control on one endpoint [View incident page](#)

win-9njrns9ohht Risk level High

NT AUTHORITY\SYSTEM

ALERT STORY

Collapse all

9:25:48 AM

[2244] SolarWinds.BusinessLayerHost.exe

Network connect

(oo) Outbound connection from 10.10.50.242:49669 to 10.10.50.199:443

Remote IP address10.10.50.199

Remote port443

Local port49669

Action timeJan 3, 2021 9:25:50 AM

Resolved Domain 3mu76044hgf7shju.appsync-api.eu-west-1.avsvmcloud.com

9:25:50 AM

[2644] cmd.exe /c pause

Network traffic to domains associated with a supply chain attack High Detected New

Process id2644

Creation timeJan 3, 2021 9:25:50 AM

Image file pathC:\Windows\SysWOW64\cmd.exe

Image file SHA1e2ead0993b917e1828a658ada0b87e01d5b8424f

Image file creation timeOct 13, 2020 11:37:56 PM

Execution detailsToken elevation: Default, Integrity level: System

User NT AUTHORITY\SYSTEM

PE metadata cmd.exe

9:25:50 AM

Suspicious process launched using cmd.exe Low Detected New

cmd.exe script interpreter process was created by SolarWinds.BusinessLayerHost.exe

Network traffic to domains associated with a supply chain attack

High Detected New

Classify this alert

True alert

False alert

Alert state

ClassificationNot Set [Set Classification](#)

Assigned toUnassigned [Assign to me](#)

Alert details

CategoryCommand and control

MITRE ATT&CK Techniques-

Detection sourceEDR

Detection statusDetected

Detection technologyBehavior,Network

Generated onJan 3, 2021 9:28:57 AM

First activityJan 3, 2021 9:25:50 AM

Last activityJan 3, 2021 9:25:50 AM

Alert description

A process has attempted to connect to domains known to serve trojanized versions of auto-update software. Connections to these domains can indicate that the machine has received a malicious update and might be under attacker control.

Recommended actions

A. Validate the alert.
1. Check the process that initiated the connection

Microsoft 365 Security

Widening the scope of the search to include all domains, the risk level is High.

ALERT STORY

[Collapse all](#)

[4284] WmiPrvSE.exe -secured -Embedding

[3340] rundll32.exe rundll32 c:\windows\legit_payload.dll EntryPoint

Suspicious behavior by a svchost.exe was observed

Medium New Detected

Process launched with the security context of another user

Low New Detected

rundll32.exe was invoked remotely

Execution typeWmi

Source machine name

Mitre techniquesT1047: Windows Management Instrumentation

Source machine ip a...

10.10.10.10

Suspicious Remote WMI Execution

Medium New Detected

rundll32.exe process was created from a remote machine 'WINDOWS10-ATP-X' using Windows Management Instrumentation (WMI)

Suspicious WMI process creation

Medium New Detected

rundll32.exe process was created from a remote machine 'WINDOWS10-ATP-X' using Windows Management Instrumentation (WMI)

Execution sourceRemote

Remote machine Ne...

Remote machine FQ...

Action timeDec 22, 2020, 6:14:58 PM

Mitre techniquesT1047: Windows Management Instrumentation

Details

Suspicious Remote WMI Execution

Medium **New**

New

[See in timeline](#) [Link to another incident](#) [Assign to me](#) [...](#)

Automated investigation 27604 triggered by this alert is: No threats found

Manage alert

ⓘ Classify this alert

True alert

False alert

Status New

New

Classification

Select classification

Alert details

Incident Multi-stage incident involving Execution & Collection on multiple endpoints ([🔗 open in Microsoft 365 Defender](#))

Detection source

EDR

Detection

Behavioral, Network

technology

Detection status	Detected
------------------	----------

Category

LateralMovement

Techniques

T1047: Windows Management Instrumentation

First activity

Dec 22, 2020, 6:14:58 PM

Last activity

Dec 22, 2020, 6:14:58 PM

Generated on

Dec 22, 2020, 6:25:50 PM




Assigned to



Automation

**Παραβίαση ADFS με την κλοπή του κλειδιού
πιστοποιητικού SAML ή με την τροποποίηση
των σχέσεων αξιοπιστίας ομοσπονδίας**

Alerts > ADFS private key extraction attempt


ADFS private key extraction attempt

  Risk level  High ...

ALERT STORY


[Collapse all](#)



[4280] SecurityHealthSystray.exe

...


▼




[7448] OneDrive.exe /background

...

▼




File create




dump_em_all.exe


...


▼




Suspicious file dropped

 Medium

 New

 Detected

...



[7956] dump_em_all.exe

...

▼






Image load




dump_em_all.exe


...


▼




Suspicious file dropped

 Medium

 New

 Detected

...




dump_em_all.exe ran an LDAP query

^


LDAP Search query

(&(thumbnailphoto=*)(objectClass=contact)(!(cn=CryptoPolicy)))



Distinguished name

CN=ADFS,CN=Microsoft,CN=Program Data,DC=ATP,DC=local



Action time

Jan 10, 2021, 7:09:02 PM



ADFS private key extraction attempt

 High


 New

 Detected

...

Details

ADFS private key extraction attempt

 High **New**

[See in timeline](#) [Link to another incident](#) [Assign to me](#) ...

Manage alert

 Classify this alert

True alert

False alert

Status

New ▼

Classification

Select classification... ▼

Alert details

Incident [Multi-stage incident involving Execution & Credential access on one endpoint \(!\[\]\(df47d6bec273bbb8b349135fff3a20f7_img.jpg\) open in Microsoft 365 Defender \)](#)

Detection source EDR

Detection technology Behavioral

Detection status Detected

Category CredentialAccess


Techniques [T1003: OS Credential Dumping](#)


Χρήση πλαστών διακριτικών SAML για τη διατήρηση στο cloud, την πρόσβαση σε πόρους cloud και την κρυφή εξαγωγή μηνυμάτων ηλεκτρονικού ταχυδρομείου.


Εντοπίστηκε ασυνήθιστος χειρισμός της εφαρμογής OAuth από το MCAS


Alerts >  **Unusual addition of credentials to an O...** 12/28/20 6:32 AM PREVIEW

+36  MEDIUM SEVERITY

 Unusual addition of credentials to an OAuth app

 Office 365

 User Name

 1.1.1.1

Resolution options:

User Name









Close alert

Description

The user User Name (username@domain.com) performed an unusual addition of credentials to App Name. This usage pattern may indicate that an attacker has compromised the app, and is using it for phishing, exfiltration, or lateral movement. The user added a credentials of type Password, where an application is using a clear text password to authenticate.

- Important information**
- Administrative activity was performed for the first time in 180 days by this user.
 - Office 365 (Default) was used for administrative activity for the first time in 180 days by this user.
 - 1.1.1.1 was used for the first time in 180 days by this user.

Activity log

1 - 3 of 3 activities ⓘ							Investigate in Activity log		
Activity	User	App	IP address	Location	Device	Date ▾			
 Update service principal: application App Name; ...	User Name	 Office 365	 1.1.1.1	 India	—	Dec 28, 2020, ...			
 Update application configuration: application Ap...	User Name	 Office 365	 1.1.1.1	 India	—	Dec 28, 2020, ...			

Microsoft 365 Security



Overview Analyst report Related incidents Impacted assets Prevented email attempts Mitigations

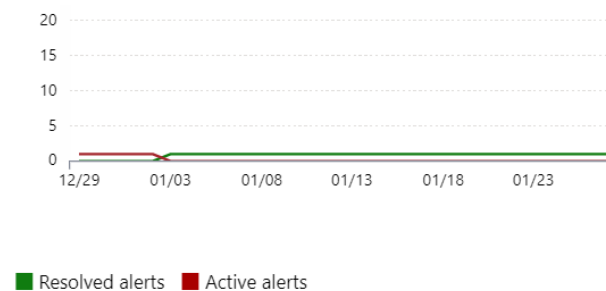
Microsoft Defender Antivirus protects against this threat. It blocks the known malicious SolarWinds binaries associated with this threat on your device.

Related incidents ⓘ

Incidents severity



Alerts over time ⓘ



Secure configuration status ⓘ

Report details

Report type	Published	Last updated
Attack campaigns	12/14/20, 7:59 AM	12/21/20, 9:38 AM

Impacted assets 

Devices 0 / 1

■ Assets with active alerts ■ Assets with resolved alerts
■ Assets with no alerts

[View all impacted assets](#)

Vulnerability patching status ⓘ

0 vulnerable devices

Microsoft 365 Security



Overview Analyst report Related incidents Impacted assets Prevented email attempts **Mitigations**

1.43k misconfigured devices



Exposed Secure Unknown Not applicable

0 vulnerable devices



Exposed Secure

Secure configuration

Vulnerabilities

Product/Component

orion_user_device_tracker

highavailability_orion_plugin

orion_netflow_traff

orion_improvement

orion_core_services

orion_network_per

orion_network_con

1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021, 2022, 2023, 2024, 2025, 2026, 2027, 2028, 2029, 2030, 2031, 2032, 2033, 2034, 2035, 2036, 2037, 2038, 2039, 2040, 2041, 2042, 2043, 2044, 2045, 2046, 2047, 2048, 2049, 2050, 2051, 2052, 2053, 2054, 2055, 2056, 2057, 2058, 2059, 2060, 2061, 2062, 2063, 2064, 2065, 2066, 2067, 2068, 2069, 2070, 2071, 2072, 2073, 2074, 2075, 2076, 2077, 2078, 2079, 2080, 2081, 2082, 2083, 2084, 2085, 2086, 2087, 2088, 2089, 2090, 2091, 2092, 2093, 2094, 2095, 2096, 2097, 2098, 2099, 2100, 2101, 2102, 2103, 2104, 2105, 2106, 2107, 2108, 2109, 2110, 2111, 2112, 2113, 2114, 2115, 2116, 2117, 2118, 2119, 2120, 2121, 2122, 2123, 2124, 2125, 2126, 2127, 2128, 2129, 2130, 2131, 2132, 2133, 2134, 2135, 2136, 2137, 2138, 2139, 2140, 2141, 2142, 2143, 2144, 2145, 2146, 2147, 2148, 2149, 2150, 2151, 2152, 2153, 2154, 2155, 2156, 2157, 2158, 2159, 2160, 2161, 2162, 2163, 2164, 2165, 2166, 2167, 2168, 2169, 2170, 2171, 2172, 2173, 2174, 2175, 2176, 2177, 2178, 2179, 2180, 2181, 2182, 2183, 2184, 2185, 2186, 2187, 2188, 2189, 2190, 2191, 2192, 2193, 2194, 2195, 2196, 2197, 2198, 2199, 2200, 2201, 2202, 2203, 2204, 2205, 2206, 2207, 2208, 2209, 2210, 2211, 2212, 2213, 2214, 2215, 2216, 2217, 2218, 2219, 2220, 2221, 2222, 2223, 2224, 2225, 2226, 2227, 2228, 2229, 2230, 2231, 2232, 2233, 2234, 2235, 2236, 2237, 2238, 2239, 2240, 2241, 2242, 2243, 2244, 2245, 2246, 2247, 2248, 2249, 2250, 2251, 2252, 2253, 2254, 2255, 2256, 2257, 2258, 2259, 2260, 2261, 2262, 2263, 2264, 2265, 2266, 2267, 2268, 2269, 2270, 2271, 2272, 2273, 2274, 2275, 2276, 2277, 2278, 2279, 2280, 2281, 2282, 2283, 2284, 2285, 2286, 2287, 2288, 2289, 2290, 2291, 2292, 2293, 2294, 2295, 2296, 2297, 2298, 2299, 2300, 2301, 2302, 2303, 2304, 2305, 2306, 2307, 2308, 2309, 2310, 2311, 2312, 2313, 2314, 2315, 2316, 2317, 2318, 2319, 2320, 2321, 2322, 2323, 2324, 2325, 2326, 2327, 2328, 2329, 2330, 2331, 2332, 2333, 2334, 2335, 2336, 2337, 2338, 2339, 2340, 2341, 2342, 2343, 2344, 2345, 2346, 2347, 2348, 2349, 2350, 2351, 2352, 2353, 2354, 2355, 2356, 2357, 2358, 2359, 2360, 2361, 2362, 2363, 2364, 2365, 2366, 2367, 2368, 2369, 2370, 2371, 2372, 2373, 2374, 2375, 2376, 2377, 2378, 2379, 2380, 2381, 2382, 2383, 2384, 2385, 2386, 2387, 2388, 2389, 2390, 2391, 2392, 2393, 2394, 2395, 2396, 2397, 2398, 2399, 2400, 2401, 2402, 2403, 2404, 2405, 2406, 2407, 2408, 2409, 2410, 2411, 2412, 2413, 2414, 2415, 2416, 2417, 2418, 2419, 2420, 2421, 2422, 2423, 2424, 2425, 2426, 2427, 2428, 2429, 2430, 2431, 2432, 2433, 2434, 2435, 2436, 2437, 2438, 2439, 2440, 2441, 2442, 2443, 2444, 2445, 2446, 2447, 2448, 2449, 2450, 2451, 2452, 2453, 2454, 2455, 2456, 2457, 2458, 2459, 2460, 2461, 2462, 2463, 2464, 2465, 2466, 2467, 2468, 2469, 2470, 2471, 2472, 2473, 2474, 2475, 2476, 2477, 2478, 2479, 2480, 2481, 2482, 2483, 2484, 2485, 2486, 2487, 2488, 2489, 2490, 2491, 2492, 2493, 2494, 2495, 2496, 2497, 2498, 2499, 2500, 2501, 2502, 2503, 2504, 2505, 2506, 2507, 2508, 2509, 2510, 2511, 2512, 2513, 2514, 2515, 2516, 2517, 2518, 2519, 2520, 2521, 2522, 2523, 2524, 2525, 2526, 2527, 2528, 2529, 2530, 2531, 2532, 2533, 2534, 2535, 2536, 2537, 2538, 2539, 2540, 2541, 2542, 2543, 2544, 2545, 2546, 2547, 2548, 2549, 2550, 2551, 2552, 2553, 2554, 2555, 2556, 2557, 2558, 2559, 2560, 2561, 2562, 2563, 2564, 2565, 2566, 2567, 2568, 2569, 2570, 2571, 2572, 2573, 2574, 2575, 2576, 2577, 2578, 2579, 2580, 2581, 2582, 2583, 2584, 2585, 2586, 2587, 2588, 2589, 2590, 2591, 2592, 2593, 2594, 2595, 2596, 2597, 2598, 2599, 2600, 2601, 2602, 2603, 2604, 2605, 2606, 2607, 2608, 2609, 2610, 2611, 2612, 2613, 2614, 2615, 2616, 2617, 2618, 2619, 2620, 2621, 2622, 2623, 2624, 2625, 2626, 2627, 2628, 2629, 2630, 2631, 2632, 2633, 2634, 2635, 2636, 2637, 2638, 2639, 2640, 2641, 2642, 2643, 2644, 2645, 2646, 2647, 2648, 2649, 2650, 2651, 2652, 2653, 2654, 2655, 2656, 2657, 2658, 2659, 2660, 2661, 2662, 2663, 2664, 2665, 2666, 2667, 2668, 2669, 2670, 2671, 2672, 2673, 2674, 2675, 2676, 2677, 2678, 2679, 26

Vulnerability IDs

TVM-2020-0002

TVM-2020-0002

devices

0

0

αναγνωριστικό ευπάθειας:
TVM-2020-0002

Security recommendations

solarwinds orion

Security recommendation	OS platform	Weaknesses	Related component	Threats	Exposed devices	Status	Remediation type
<div><div></div><div>Update Solarwinds Orion Network Performance Monitor</div></div>	Windows	2	Solarwinds Orion ...	<div><div></div><div></div><div></div></div>	7 / 8	<div><div></div></div> Active	Software update
Update Solarwinds Orion Core Services	Windows	1	Solarwinds Orion ...	<div><div></div><div></div><div></div></div>	4 / 12	<div><div></div></div> Active	Software update
Update Solarwinds Orion Network Configuration Manager	Windows	1	Solarwinds Orion ...	<div><div></div><div></div><div></div></div>	1 / 6	<div><div></div></div> Active	Software update

Update Solarwinds Orion Network Performance Monitor

[Open software page](#)
[Remediation options](#)
[Exception options](#)

Description

Update Orion Network Performance Monitor to a later version to mitigate 2 known vulnerabilities affecting your devices.

Vulnerability details

Number of vulnerabilities

Exploit available

No

Exposed devices

7/8

Exposed operating systems

Windows Server 2016, Windows Server 2012 R2

Νέα δεδομένα Azure Active Directory και εφαρμογής Cloud στον Σύνθετο εντοπισμό

Advanced hunting

Schema

Alerts

- AlertInfo
- AlertEvidence

Apps & identities

- IdentityInfo
- IdentityLogonEvents
- IdentityQueryEvents
- IdentityDirectoryEvents
- AppFileEvents
- CloudAppEvents
- AADSpnSignInEventsBeta
- AADSignInEventsBeta**

Timestamp
Application
ApplicationId
LogonType
ErrorCode
CorrelationId
SessionId
AccountDisplayName
AccountObjectId
AccountUpn
IsExternalUser
IsGuestUser
AlternateSignInName
LastPasswordChangeTimestamp
ResourceDisplayName
ResourceId

Get started

Query

Run query

+ New

Save

Share link

```
1 //Look for throttled mailboxes which indicates excessive mail access over a short period of time
2
3 let starttime = 2d;
4 let endtime = 1d;
5 CloudAppEvents
6 | where Timestamp between (startofday(ago(starttime))..startofday(ago(endtime)))
7 | where ActionType == "MailItemsAccessed"
8 | where isnotempty(RawEventData["ClientAppId"]) and RawEventData["OperationProperties"][1] has "True"
9 | project Timestamp, RawEventData["OrganizationId"], AccountObjectId, UserAgent
```

Export

Timestamp RawEventData.OrganizationId AccountObjectId UserAgent

No results found in the specified time frame.

AADSignInEventsBeta

Description

Information about Azure Active Directory (AAD) sign-in events either by a user (interactive) or a client on the user's behalf (non-interactive)

Columns

Fields in this table:

Timestamp

Date and time when the record was generated

Application

Application that performed the recorded action

ApplicationId

Unique identifier for the application

[View all](#)

Sample queries

[Sign-ins to disabled accounts](#)

[Users signing in from multiple locations](#)

CloudAppEvents
/ where Application == "Office 365"

[See full documentation](#)

Διερεύνηση ειδοποιήσεων και περιστατικών που σχετίζονται με το Solorigate στο Microsoft 365 Defender

Incidents > Multi-stage incident involving Execution & Collection on multiple endpoints

[Manage incident](#) [? Consult a threat expert](#) [Comments and history](#)

Summary Alerts (50) Devices (2) Users (3) Mailboxes (0) Investigations (6) Evidence (154)

Alerts and categories

50/50 active alerts
7 MITRE ATT&CK tactics
2 other alert categories















© 2018 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation

- Dec 22, 2020, 1:52:20 AM | **New**
A WMI event filter was bound to a suspicious event consumer on Desktop-3456789
- Dec 22, 2020, 11:08:57 AM | **New**
Process launched with the security context of another user on Win-9012345678
by user mntd000p
- Dec 22, 2020, 11:37:49 AM | **New**
Suspicious file deletion activity was observed on Win-9012345678: by user mntd000p
- Dec 22, 2020, 11:58:50 AM | **New**
Scheduled task possibly hijacked on Win-9012345678: by user mntd000p
- Dec 22, 2020, 11:58:50 AM | **New**
Suspicious remote activity on Win-9012345678: by user mntd000p
, and more.
- Dec 22, 2020, 11:58:50 AM | **New**
Suspicious file creation initiated remotely on Win-9012345678: by user

Scope

2 impacted devices
3 impacted users

Top impacted entities

Entity type	Risk level/investigation priority	Tags
 	 High	
 	 High	
 	No data available	
 	No data available	
 	No data available	

View entities

Evidence

154 entities found

Evidence remediation status

[View all entities](#)

Incident Information

(i) This incident might be associated w...

Associated incidents

Incident ID	Reason	Entity
24851	Same file	sqlceip.exe
24576	Same file	legit_payl...
24576	Same file	payload.dll

Tags summary

Incident tags

Incident details

Status

Active

Severity

■■■ High

Incident ID

24963

First activity

First - Dec 22, 2020, 1:52:20 AM

Last activity

Last - Dec 28, 2020, 3:04:12 PM

Classification

Not set

Determination

Not set

Σειρά βίντεο Solorigate

Επόμενα βήματα

- 01.** Παρακολουθήστε τη σειρά βίντεο Solorigate σε αυτήν την τοποθεσία
- 02.** Επισκεφθείτε την Ασφάλεια της Microsoft για περισσότερες ενημερώσεις: www.microsoft.com/en-us/security/business
- 03.** Διαβάστε τις δημοσιεύσεις ιστολογίου στη διεύθυνση: www.microsoft.com/security/blog

<https://aka.ms/solorigate>

