encode
cyber threat management

Managed Detection & Response

leveraging Microsoft Defender for Endpoint

Manage the threats that matter most

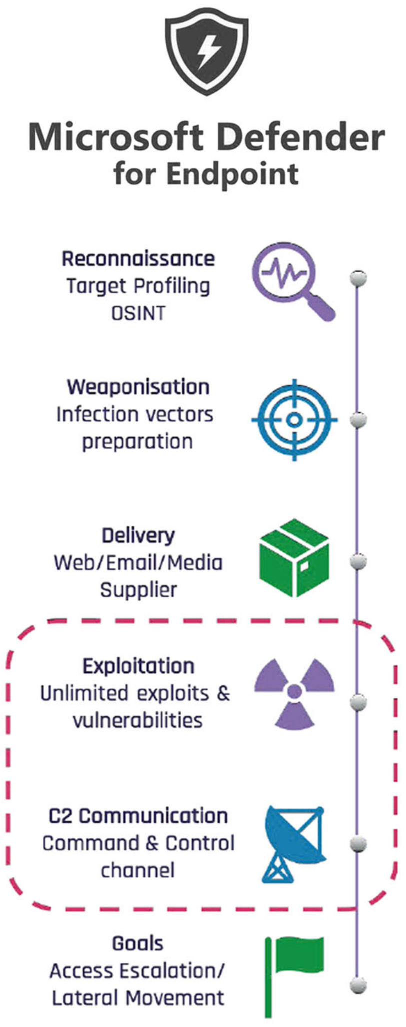
Companies of virtually any size and in every sector can find themselves being the target of offensive cyber operations, be it cyber-crime, state-sponsored or competition-sponsored attacks, targeted ransomware and supply-chaincompromises. The common denominator in most of these incidents, regardless of actor's motives, is the establishisment of a foothold inside the target's digital enviroment. Once the latter has been achieved, the attackers try to obtain further access and ultimately compromise one or more IT assets (endpoints) for establishing command and control (C2) channel(s) with the CnC center. Encode's 18+ years of experience in simulating such attacks through our Red Team exercises and responding to them, show that early detection and timely, coherent response is of paramount importance for minimizing business impacts.

Encode MDR solution

Encode's MDR service is designed to enable Early Breach Detection and Adaptive Response against endpoint compromise-related threats. Whether you use Cloud/SaaS, hosted or in-house business applications and IT services, your endpoints are the target and your user-population is theweakest link, requiring 24x7 proactive protection with Detection and Response capabilities as a managed service.

Encode MDR does not rely on low visibility sources already present in the monitored environment, such as existing system log sources, but rather utilizes the unique capabilities of **Microsoft Defender for Endpoint** together with Enorasys Platform for maximum visibility and minimum footprint possible. Encode's MDR service provides:

- 24x7 Cyber SOC Operations.
- On-going endpoint threat hunting, detection & response using MS Defender for Endpoint EDR capabilities and behavioral rules.
- Continuous automated hunting of C2 channels to detect unknown, evasive attacks (APT) using Enorasys Security Analytics.
- SOAR-based incident investigation, scoping and adaptive response using Enorasys SOCStreams.
- A powerful integration and workflow engine enabling the automation of incident investigation and response activities (playbooks).
- A complete customer/service portal providing full Incident Handling visibility, real-time collaboration and SLA/KPI reporting.



Microsoft Defender for Endpoint

Reconnaissance
Target Profiling
OSINT

Weaponisation
Infection vectors
preparation

Delivery
Web/Email/Media
Supplier

Exploitation
Unlimited exploits &
vulnerabilities

C2 Communication
Command & Control
channel

Goals
Access Escalation/
Lateral Movement

encode
cyber threat management

MDR Service with MS Defender for Endpoint
Key Features

End to End Detection and Response

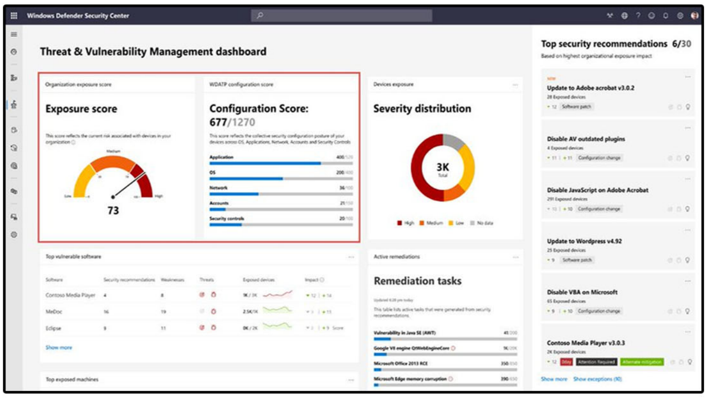
With Encode's MDR service you don't get just a provider handing over possible cases to your team, but rather an end-to-end detection and response solution, with all the tools pre-deployed and integrated to cover the entire process of *'Breach Indicators Generation – Assessment and in-depth Investigation – Incident Scoping/Hunting – Containment'*, on a 24x7 basis, while collaborating with your team and providing guidance for complete threat eradication and recovery.

24x7 Cyber Threat Hunting and Response

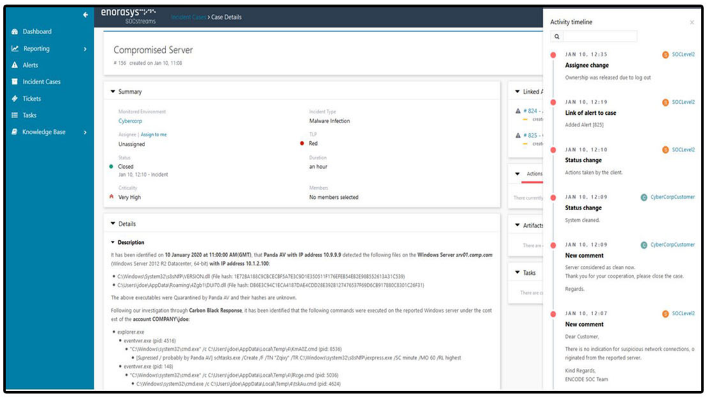
Encode's analytics and proprietary behavioral rule-sets continuously generate "breach indicators"; such indicators constitute a "high accuracy" hypothesis setting triggers for the 24x7 threat-hunting team to initiate targeted investigations and hunting processes for cotinuous identification of breaches, very early in the attack kill chain.

MDR-focused tech stack

To support an effective MDR solution our tech stack was designed and built from the ground-up for being a true enabler and force-multiplier to our team of experts. Enorasys SOCStreams, our proprietary SOAR platform, is the focal point of our solution, providing the tools to our analysts to assess breach indicators, perform targeted investigation, incident scoping, hunting and response actions. On top of that our Enorasys Security Analytics platform provides continuous profiling and analysis of all outbound Internet activity enabling the automated hunting of C2 channels, while MS Defender for Endpoint provides the necessary threat hunting, detection and response capabilities at the endpoint level. The combination of these three technology components supported by a series of backend analytics and threat intelligence tools are used for connecting the dots to attack paths, by mapping and correlating different indicators on the cyber kill-chain as well as for analyzing attack artifacts and threat actors.



Windows Defender Security Center
Threat & Vulnerability Management dashboard
Organization exposure score
Exposure score
This score reflects the current risk associated with devices in your organization
Medium
Low
High
73
WDATP configuration score
Configuration Score:
677/1270
This score reflects the collective security configuration posture of your devices across OS, Applications, Network, Accounts and Security Controls
Application
OS
Network
Accounts
Security controls
Devices exposure
Severity distribution
3K
Total
High
Medium
Low
No data
Top vulnerable software
Software
Security recommendations
Weaknesses
Threats
Exposed devices
Impact
Contoso Media Player
MeDoc
Eclipse
Show more
Active remediations
Remediation tasks
This table lists active tasks that were generated from security recommendations.
Vulnerability in Java SE (AWT)
Google V8 engine QtWebEngineCore
Microsoft Office 2013 RCE
Microsoft Edge memory corruption
Top exposed machines
Top security recommendations 6/30
Based on highest organizational exposure impact
Update to Adobe acrobat v3.0.2
28 Exposed devices
Software patch
Disable AV outdated plugins
4 Exposed devices
Configuration change
Disable JavaScript on Adobe Acrobat
291 Exposed devices
Configuration change
Update to Wordpress v4.92
25 Exposed devices
Software patch
Disable VBA on Microsoft
65 Exposed devices
Configuration change
Contoso Media Player v3.0.3
2K Exposed devices
Attention Required
Alternate mitigation
Show more
Show exceptions (90)



Compromised Server
156 created on Jan 10, 11:08

Summary

Monitored Environment: Cybercorp
Incident Type: Malware Infection
Assignee | Assign to me: Unassigned
TLP: Red
Status: Closed, Jan 10, 12:10 - Incident
Duration: an hour
Criticality: Very High
Members: No members selected

Details

Description

It has been identified on **10 January 2020 at 11:00:00 AM(GMT)**, that **Panda AV with IP address 10.9.9.9** detected the following files on the **Windows Server** ***srv01.comp.com*** (Windows Server 2012 R2 Datacenter, 64-bit) **with IP address 10.1.2.100**:

- C:\Windows\System32\s8sNfP\VERSION.dll (File hash: 1E728A188C9CBCECBF5A7E3C9D1E350511F176EFEB54EB2E98B552613A31C539)
- C:\Users\jdoe\AppData\Roaming\4Zgb1\DUI70.dll (File hash: DB6E3C94C1ECA4187DAE4CDD28E392B127476537F69D6CB917880C8301C26F31)

The above executables were Quarantined by Panda AV and their hashes are unknown.

Following our investigation through **Carbon Black Response**, it has been identified that the following commands were executed on the reported Windows server under the context of the **account COMPANY\jdoe**:

- explorer.exe
  - eventvwr.exe (pid: 4516)
    - "C:\Windows\system32\cmd.exe" /c C:\Users\jdoe\AppData\Local\Temp\4\KmA0Z.cmd (pid: 8536)
      - [Supressed / probably by Panda AV] schtasks.exe /Create /F /TN "Zqixy" /TR C:\Windows\system32\s8sNfP\iexpress.exe /SC minute /MO 60 /RL highest
  - eventvwr.exe (pid: 148)
    - "C:\Windows\system32\cmd.exe" /c C:\Users\jdoe\AppData\Local\Temp\4\lRcge.cmd (pid: 5036)
      - C:\Windows\system32\cmd.exe /c C:\Users\jdoe\AppData\Local\Temp\4\tskAu.cmd (pid: 4624)

JAN 10, 12:35 — SOCLevel2
Assignee change
Ownership was released due to log out

JAN 10, 12:19 — SOCLevel2
Link of alert to case
Added Alert [825]

JAN 10, 12:10 — SOCLevel2
Status change
Actions taken by the client.

JAN 10, 12:09 — CyberCorpCustomer
Status change
System cleaned.

JAN 10, 12:09 — CyberCorpCustomer
New comment
Server considered as clean now.
Thank you for your cooperation, please close the case.
Regards.

JAN 10, 12:07 — SOCLevel2
New comment
Dear Customer,
There is no indication for suspicious network connections, originated from the reported server.
Kind Regards,
ENCODE SOC Team

enorasys SOCstreams | Microsoft Defender for Endpoint | enorasys Security Analytics

encode
cyber threat management

About ENCODE:

Encode specializes on Targeted Cyber Threats and stands out with its proprietary technology, expertise on cyber security and multiyear experience across vertical industries, coupled with on-going, innovative security research and its highly qualified and talented people. With global operations and local expertise, Encode combines its cutting edge technology with best of breed Cyber Security Operations and Services to augment its clients' cyber security capabilities for the continuous and effective management of advanced cyber threats.