DETECTING CONTI RANSOMWARE

with Ordr

ordr

NOTICES

CONTENTS

INTRODUCTION

The FBI Cyber Division on 20th May 2021 identified at least 16 Conti ransomware attacks over the past year.

Targets included:

- U.S. healthcare and first responder networks,
- law enforcement agencies,
- emergency medical services,
- 9-1-1 dispatch centers, and municipalities.

The FBI also stated that the Conti ransomware gang targeted close to 400 first responder networks worldwide; close to 290 of these organizations are located in the U.S. The average payment for Conti ransomware was $782,636, and systems were taken offline for an average of 14 days. This ransomware gang has recently breached Ireland's Health Service Executive (HSE) networks and Department of Health (DoH), asking the former to pay a $20 million ransom after successfully encrypting its systems.

See the documentation at the following references:

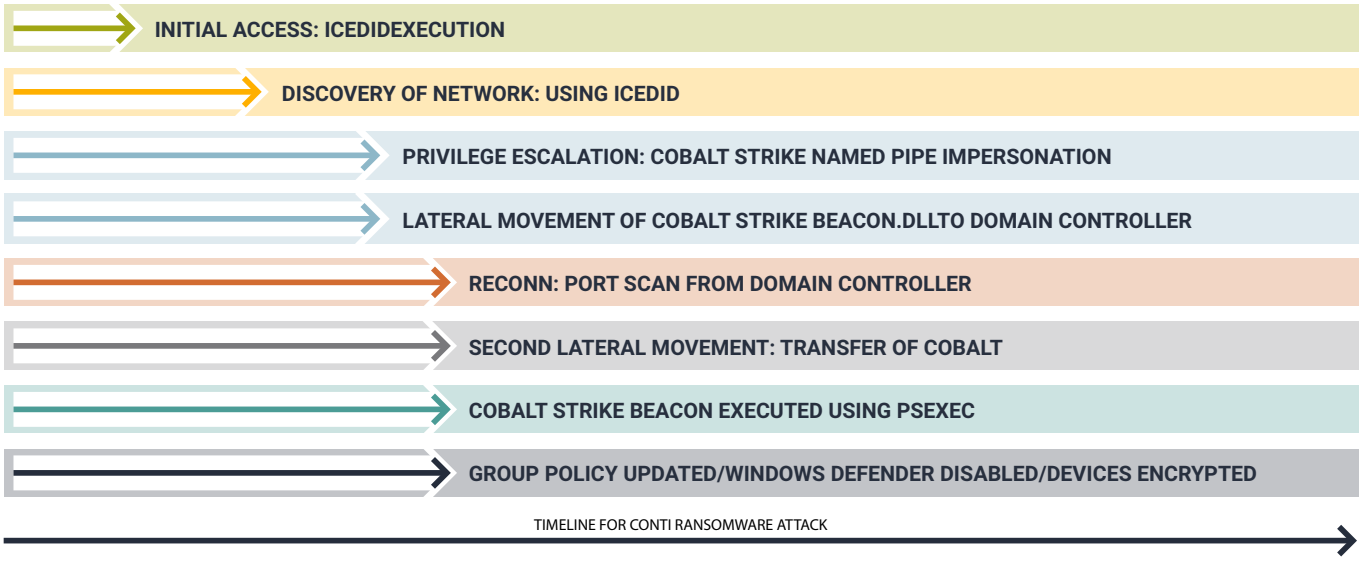
- https://www.coveware.com/conti-ransomware
- https://www.bleepingcomputer.com/news/security/irelands-health-services-hit-with-20-million-ransomware-demand/

WHAT IS THE CONTI RANSOMWARE GANG?

Conti ransomware is a private Ransomware-as-a-Service (RaaS) controlled by a cyber gang, Wizard Spider. Conti shares some of its code with Ryuk ransomware and uses the same TrickBot distribution channels and Cobalt Strike beacons after Ryuk activity decreased around July 2020.

TIMELINE OF CONTI RANSOMWARE

The Conti Ransomware infection will follow the timeline shown in the following diagram:



DETECTION OF CONTI USING ORDR

Ordr SCE (Systems Control Engine) uses multi-faceted data to calculate the risk and security posture of every individual device in the protected network. The Ordr platform uses deep packet inspection to capture device data, including:

- **Static attributes such as O.S. information of the device,**
- **Hotfixes deployed,**
- **Applications deployed,**
- **And the behavioral patterns of the device.**

Ordr security capabilities includes an integrated Threat Detection Engine to detect exploits and lateral movement, and industry-leading threat intelligence to detect more than 1000 critical event types that point to vulnerable devices in the network. In addition, Ordr uses AI to map and baseline every device communications flow, complete with risk scores, to detect anomalous traffic.

The Ordr SCE solution includes the SCE Analytics Engine, and the Ordr SCE Sensors. The SCE Analytics Engine collects information in the Ordr Data Lake and processes it with machine learning and continuous analytics.. The Ordr SCE Sensors inspects network traffic and sends metadata to SCE.

The following sections describe how Ordr SCE detects Conti Ransomware in its various phases.

DETECTION OF INITIAL ACCESS

Ordr SCE updates threat intelligence in real-time, and all communications with the IcedID IoC list* are marked risky.

```
vaclicinn.xyz
thulleultinn.club
oxythuler.cyou
dictorecovery.cyou
expertulthima.club
68.183.20.194:80
159.89.140.116:443
83.97.20.160:443
```

**IoCs obtained from:*

- https://thedfirreport.com/2021/05/12/conti-ransomware/
- https://otx.alienvault.com/pulse/5f0781369d8978954c40d9f1

DETECTION OF LATERAL MOVEMENT

Ordr sensors deployed across the network include an integrated Threat Detection Engine that monitors all ingress-egress and east-west traffic and alerts on malicious activity and anomalous communication behavior. In the case of Conti, Ordr can detect the "Cobalt Strike " lateral movement.

Ordr SCE analyzes and baselines the traffic based on expected behavior, and any deviation from this normal traffic is marked as anomalous on the system.

DETECTION OF EXFIL

Ordr sensors deployed across the network include an integrated Threat Detection Engine that monitors all ingress-egress and east-west traffic, including detection of a complete suite of reconnaissance attacks like port scanning used to detect vulnerable devices in the network. Conti ransomware uses recon from domain controllers to detect vulnerable devices. The secondary transfer is based on the reconnaissance attack.

Ordr threat Intelligence can detect all I.P./URLs** marked for Conti domains as risky communications and increase the risk score of the device accordingly.

```
tapavi.com
ontirecovery.best
us/ky/louisville/312-s-fourth-st.html
23.106.160.174
23.82.140.137
```

***IoCs obtained from:*

- https://thedfirreport.com/2021/05/12/conti-ransomware/
- https://otx.alienvault.com/pulse/5f0781369d8978954c40d9f1

PREVENTING RANSOMWARE ATTACKS

Ordr SCE is a tool that provides complete visibility into all the connected assets in the enterprise. All assets are assigned a risk score, which is a measure of the riskiness of the device. In ransomware, all the devices that exhibited the above patterns will have a risky score level of critical and high. This will allow users to easily track and remediate these devices.

Ordr has the most comprehensive integrations in the industry, including deep integration with the firewalls and NAC vendors for immediate, automated response. Users will have an option to quarantine the devices based on the risky level or detection of any security event or behavior anomaly that point to a possibility of an attack in the enterprise.

INFO@ORDR.NET WWW.ORDR.NET 2445 AUGUSTINE DRIVE SUITE 601, SANTA CLARA, CA 95054