Introduction

A CSIRT team member has identified an attack on the SIEM called RYUK

The objective is to Investigate the attack by answering the following questions

Create a report with initial findings for the team to start formulating a plan and/ or playbook for this threat.

Threat Background and Investigation

Find the relevant Advisory and Threat report from the National Cybersecurity Centre (UK)

What are the titles of these reports?

Other resources of Threat intelligence may be available from:

The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA

Investigate the attack and answer the following questions:

How does it send and receive data ?

What is the malware that infects the users ?

How does it deploy malicious scripts ?

How much ransom is demanded ?

Which IP addresses are currently tracked as online botnet Command&Control servers (C&Cs) ?

What is the botnet used by Ryuk ?

Make a list and brief summary of ebanking trojans

Threat Indicators

What are the Indicators of compromise of Ryuk including hashes ?

Using file reputation service find which IOCs have antivirus detection ?

What is Cisco Talos Intelligence File reputation information of the IOC ?

What Encryption does RYUK Ransomeware use ?

What themes were used to entice users to click on malicious attachments?

What threat actor or actors are behind Ryuk ?

What are the webpages to find Mitre ATT&CK Techniques for Emotet and Trickbot?

Detection and Mitigation

What are the NCSC guidelines for Mitigation of Ryuk?

Where can I find the Snort / Suricata rule set to check for Emotet malware distribution sites?

What IP addresses should I block to stop the network contacting C and C (C2) servers ?

According to the latest analysis in January 2022 What domains are contacted by the scripts used in the webinject module of the trickbot trojan?

Wireshark analysis

This tutorial describes a packet capture analysis of the threat we are investigating

https://unit42.paloaltonetworks.com/wireshark-tutorial-examining-trickbot-infections/

This tutorial describes the display filters required for threat analysis in wireshark

https://unit42.paloaltonetworks.com/using-wireshark-display-filter-expressions/

Download the pcap from this page. The pcap is contained in a password-protected zip archive named ***2019-09-25-Trickbot-gtag-ono19-infection-traffic.pcap.zip***. Extract the pcap from the zip archive using the password ***infected*** and open it in Wireshark.

Find a threat report on the file contained in the payload : invoiceandstatement.lnk

Warning this file is Malware You do not need to extract this file from its zipped archive you can analyse the reputation of the hash of the zipped archive.

What is the login credentials for the gmail account of Randy Bachmann?

Resources

National Cyber Security Centre UK

Cybersecurity and Infrastructure security Agency USA

Alienvault - Open Threat Exchange OTX

Microsoft Security blog 2020

McAffee – Threat Centre Dashboard analysis F5

Labs Threat intelligence www.malware-traffic-analysis.net

Cisco - Talos Intelligence

Malwarebytes Blog