CYBER DIVISION

FEDERAL BUREAU OF INVESTIGATION

Ransomware

Gabriel Gundersen
Supervisory Special Agent,
Portland Field Office

UNCLASSIFIED

Legal Disclaimer

- The views and opinions of the presenter are personal to the presenter and do not necessarily reflect the official policy or position of any agency of the U.S. Government.
- This presentation should not be considered or construed as legal advice on any individual matter or circumstance.
- The contents of this document are intended for general information purposes only and may not be quoted or referred to in any other presentation, publication or proceeding without the prior written consent of the FBI.

Overview

- Background/History
- Impact
- Prevention, Protection, and Response
- Role of the FBI

What is Ransomware?

Ransomware is a malware that encrypts a user's files and computers, making them inaccessible until a ransom is paid.

- Victim's computer is infected with the malware.
- Encrypts victim's data and/or systems, making them unreadable.
  - Networked backups are encrypted or deleted
- Announces Itself unlike other malware
  - Actor demands payment to decrypt files or network.
  - Cryptocurrency (BTC)
- Constantly evolving
  - People pay
  - Enterprise attacks on the rise

Ransomware Background

- Modern day ransomware began around 2013
  - Cryptolocker
  - Ransoms were $300 - $700

- Primary Actors Deploying Ransomware
  - Cyber-criminals
  - Financially motivated

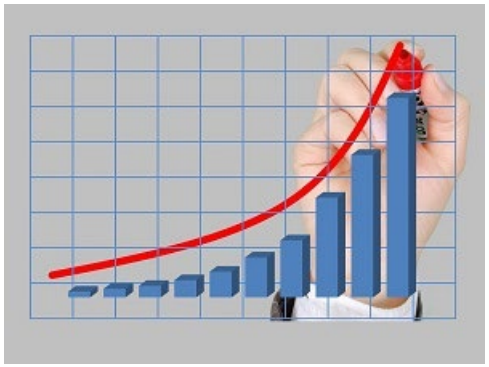
- Difficult to investigate
  - All aspects are supported by anonymization
  - Initial intrusion
  - TOR (Darkweb)
  - Virtual Currency

Ransomware Statistics

- FBI Internet Criminal Complaint Center (IC3)
  - 2016 = 2,673
  - 2017 = 1,783
  - 2018 = 1,498
  - 2019 = 1,934
  - 2020 = 2,372
  - 2021 = 2,414 (projected: 3421)
    - As of 09/14/2021

Global Impact

- Government, Health, Emergency Services, Hospitals, Police & Fire
- Loss of critical work
  - City records/planning documents, LE evidence, DNA
  - Patient Records, imaging, degradation of care
  - 911 dispatch and EMS response
- Remediation Costs
  - Can be in the millions



- 80% of victims who paid a ransom were targeted AGAIN – 50% of the time by the same actors
- Paying a ransom vs not
  - FBI recommendation

Global Impact Costs

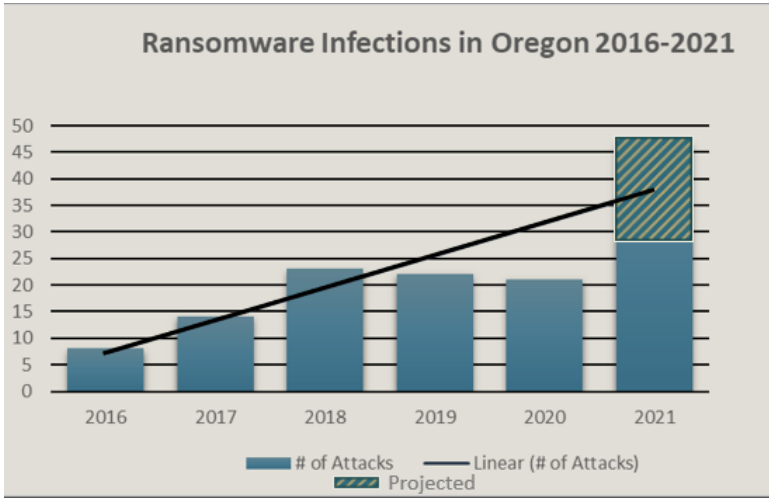
- Risk to Government, Health, and Emergency Services
  - UK NHS: $120M
  - Baltimore: $18M
  - Alabama/Texas Hospitals

- Private Sector Impact
  - Danish Co: $80M
  - Maersk/FEDEX: $300M

Oregon Impact

- As of mid September 2021, 2414 IC3 complaints, 32 in Oregon[1]
- Average Ransom Demand = $36,000 (2019) $847,344 (2020)

- Non-Ransom Costs:
  - $900,000 Average Cost for Small Companies[2]
    - Remediation
    - Legal Fees
    - Lost business
    - Downtime
  - Larger companies paying in multi-millions
  - Most costs must be paid even if you pay ransom!!
- Oregon attacks typically 4 per month



- Top targets: medical, government, academics, manufacturing, retail, technology

1. Source: IC3, as of 14 September 2021
2 Source: https://threatpost.com/ransomware-a-persistent-scourge-requiring-corporate-action-ow/145731/##targetText=A%20ransomware%20attack%20will%20be, remediation%2C%20legal%20costs%20and%20more

Mitigation/Recovery From Ransomware

- Offline Backups
  - Networked vs Offline
  - Backup regularly and often
  - Restore procedures
- Identify and fix the underlying problem
  - Employee Training/Awareness
  - Vulnerability Testing
- Contact the FBI
  - Basic reporting requests
  - Decryption capabilities in limited circumstances

What is the FBI Doing About Ransomware?

- Hold actors accountable
- Target the criminal ecosystem
- Outreach/education

THE UNITED STATES DEPARTMENT of JUSTICE

Search this site

ABOUT | OUR AGENCY | PRIORITIES | NEWS | RESOURCES | CAREERS | CONTACT

Home » Office of Public Affairs » News

SHARE

JUSTICE NEWS

Department of Justice

Office of Public Affairs

RELATED LINKS

Speeches and Press Releases

Videos

Photos

FOR IMMEDIATE RELEASE

Monday, August 13, 2018

Washington State Man Sentenced to Prison for Role in Connection with Reveton Ransomware

A former Microsoft employee was sentenced today to 18 months in prison after pleading guilty to conspiracy to commit money laundering in connection with the spread of a particular type of ransomware commonly referred to as Reveton.

Assistant Attorney General Brian A. Benczkowski of the Justice Department's Criminal Division, U.S. Attorney Benjamin C. Greenberg for the Southern District of Florida and Special Agent in Charge Matthew J. DeSarno of the FBI Washington Field Office's Criminal Division made the announcement.

Raymond Odigie Uadiale, 41, of Maple Valley, Washington, was sentenced by U.S. District Court Judge William P. Dimitrouleas for the Southern District of Florida following his June 4 guilty plea. The indictment charged Uadiale with one count of conspiracy to commit money laundering and one count of substantive money laundering. As part of the plea agreement, the government dismissed the substantive count. In addition to his prison sentence, Uadiale was also sentenced

Incident Reporting

www.IC3.gov

CYWATCH@fbi.gov
(855) 292-3937

Questions

Gabriel Gundersen
Supervisory Special Agent
Oregon Cyber Task Force
Portland Field Office, FBI
grgundersen2@fbi.gov, (503) 224-4181