



UPU | UNIVERSAL  
POSTAL  
UNION

POC C 1 PSG ITSEP 2020.1–Pres 4

# Ransomware: response and resiliency

Presentation by United States of America  
Timothy J. Shimeall, Ph.D.  
Software Engineering Institute  
Carnegie Mellon University



Copyright 2020 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University. FedEx and logo are registered in the US Patent and Trademark Office by FedEx Corporation.

DM20-0484

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.



UPU

UNIVERSAL  
POSTAL  
UNION

## Overview

Ransomware

Identify

Protect

Detect

Respond

Recover

Decisions



Attack holding data from a compromised computer

- Encrypt data
- Threaten loss or disclosure
- Demand payment
- Repeated attack

Attacks growing against organizations, not individuals

In 2019, Internet Crime Coordination Center report:

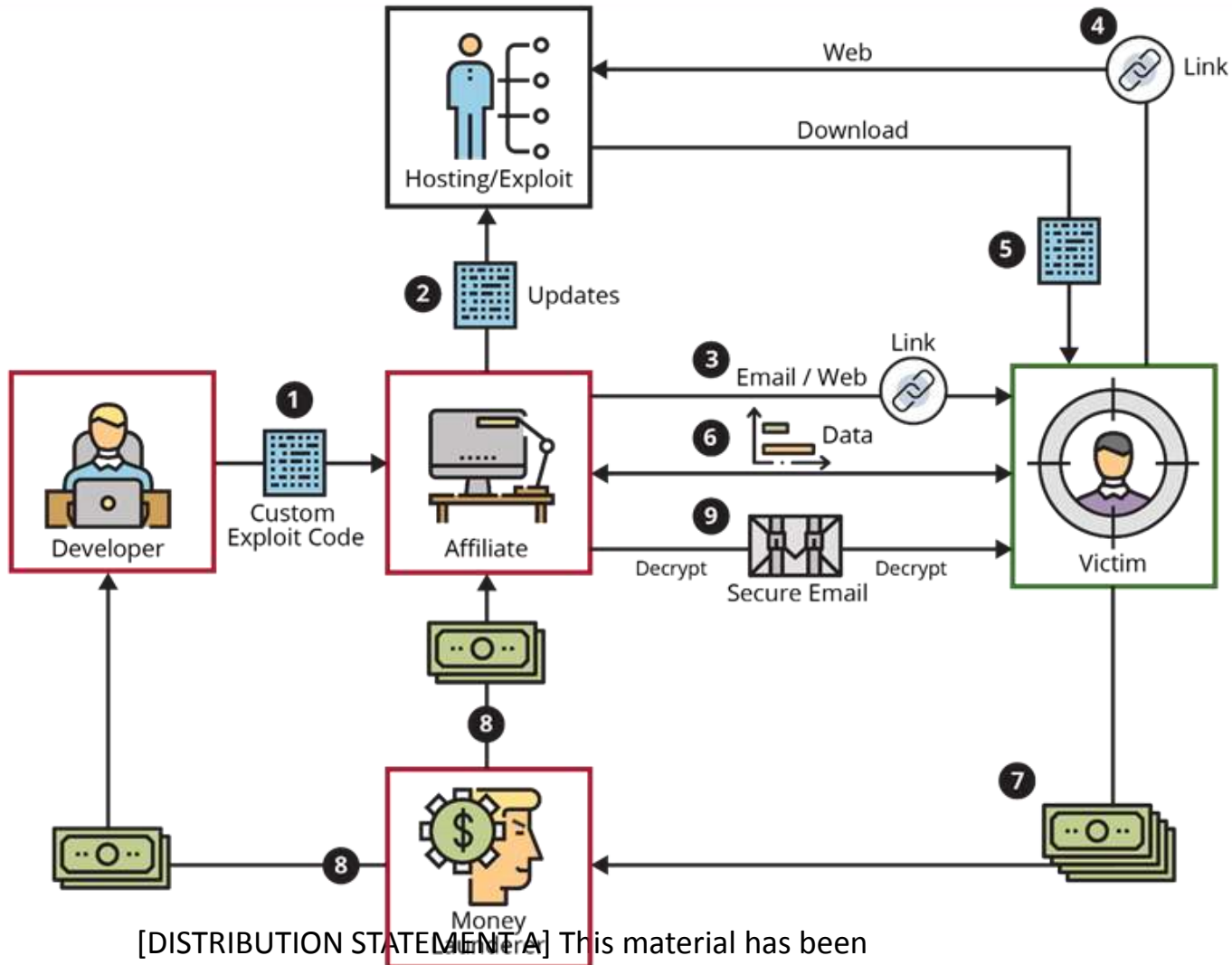
- 2,047 complaints
- US \$8,965,847 losses

In 2018, SentinelOne (UK) report:

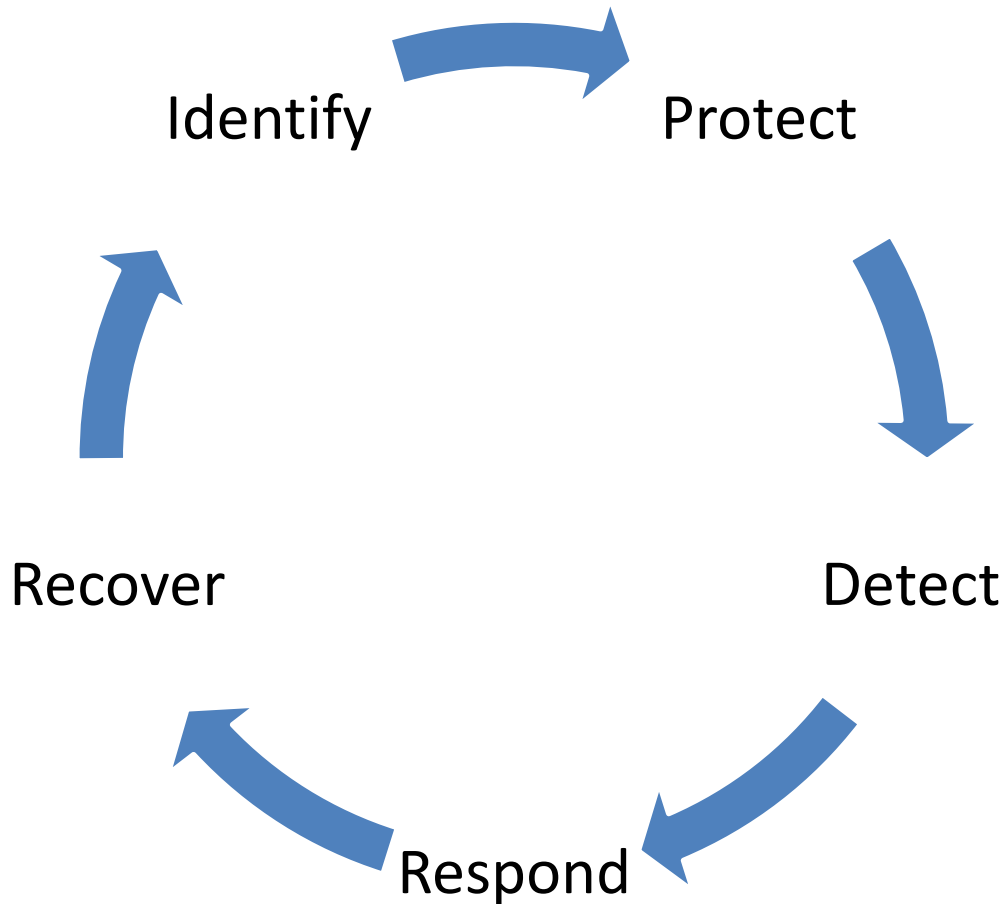
- Average attacked organization: 5 attacks in 12 months



# Ransomware Attack



[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.





### Assets

- Devices, Clients, Servers, Data
- Processing platforms, Applications
- Documentation

### Vectors

- Malware propagation methods, Access paths
- Downstream risk to assets

### Priority

- Business value, criticality
- Allocate resources in line with risk, priority



## Identify Example

Corrupted software  
update



Infected



Identification is ongoing

Include all paths to assets

Examine expected paths



Lost or redirected packages  
US \$300,000,000 loss  
Reputation loss



UPU

UNIVERSAL  
POSTAL  
UNION

## Protect

Backups

Security Hygiene

Social Engineering  
Defenses

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.



## Phishing

To: Postal Agent  
From: [orders@example.com](mailto:orders@example.com)

Attached is the invoice for  
your shipment

Malware

## Postal Agent

Did not open malware  
Closed critical file shares

Reported message to  
Security

Data

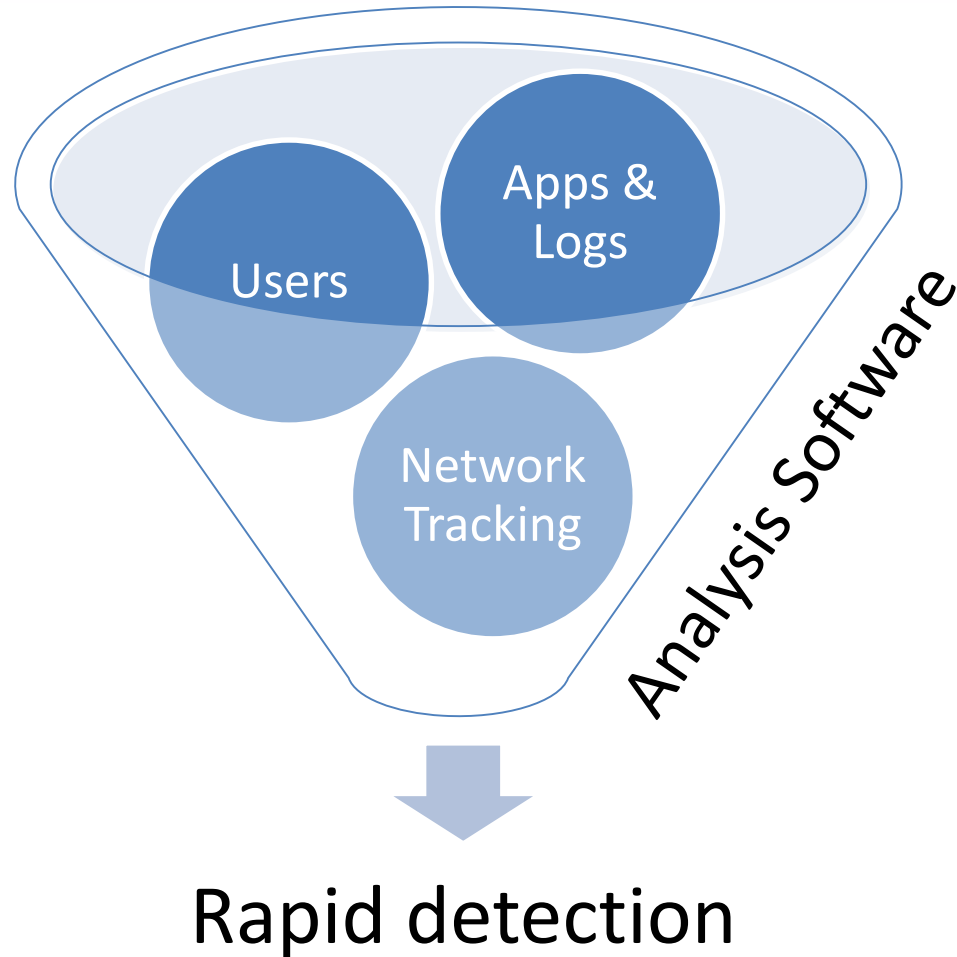
## Security

Analyzed malware  
Warned clients and vendors  
Updated defenses

Reported message to Law  
Enforcement



## Detect





### Ryuk

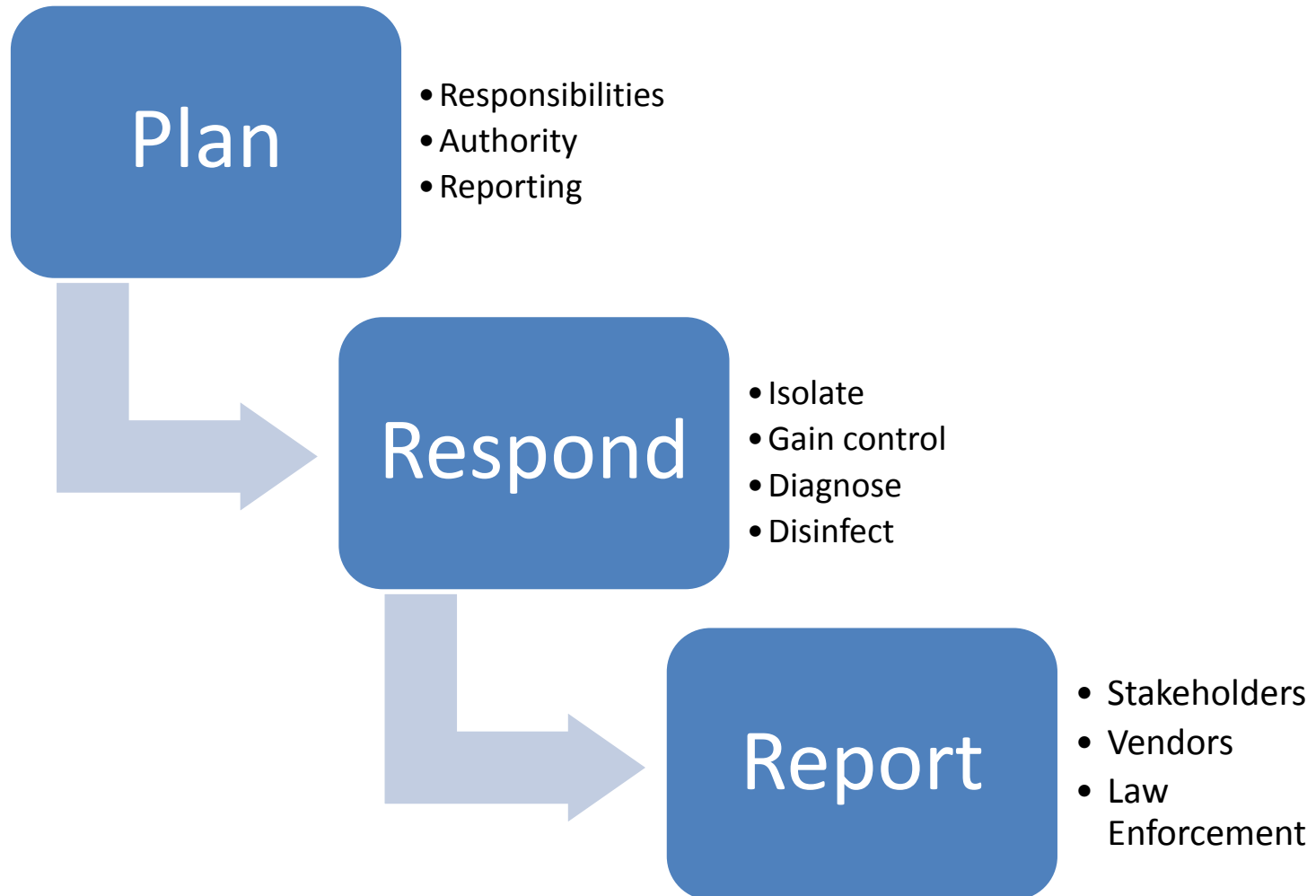
- Social engineering attacks (phishing or user click)
- Insecure web site attacks
- Invoke Trickbot and Emotet

### Trickbot and Emotet

- Spread using PsExec or Group Policy update
- Drop Ryuk
- Gain RDP access
- Steal data
- Make network more vulnerable to later Ryuk attacks



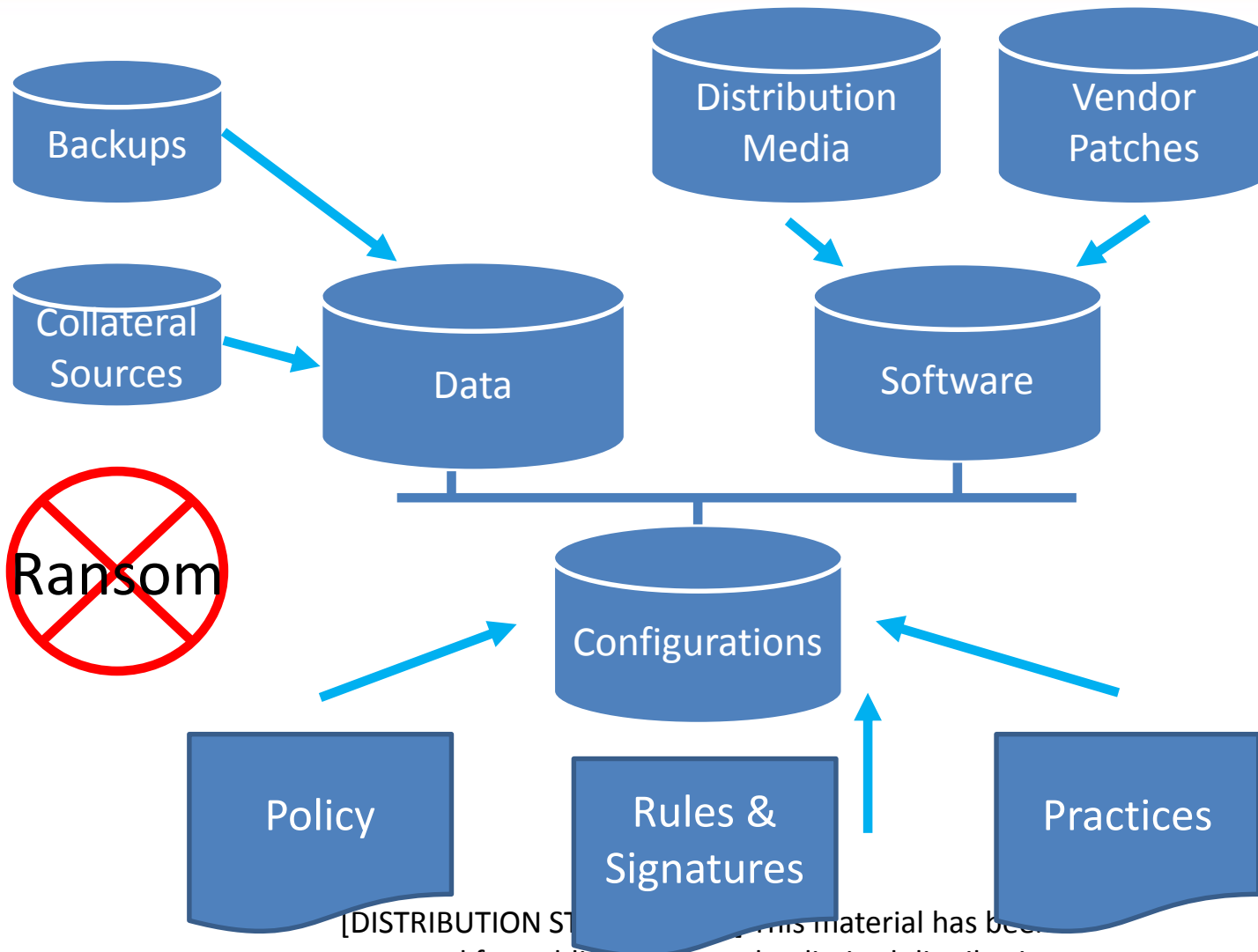
## Respond



[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.



# Recover



[DISTRIBUTION STATEMENT] This material has been approved for public release and unlimited distribution.



## Decisions expected

- Allocating resources
- Emphasizing strategies
- Moving forward