US-CERT | United States Computer Emergency Readiness Team

BEST PRACTICES AND COMMON MISSTEPS IN RESPONDING TO MAJOR INCIDENTS

Chris Butera
Chief of Incident Response,
US-CERT

Homeland Security

DISCLAIMER

This presentation is intended for informational and discussion purposes only.

The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding this information. In no event shall the United States Government or its contractors or subcontractors be liable for any damages, including but not limited to, direct, indirect, special or consequential damages, arising out of, resulting from, or in any way connected with this information, whether or not based upon warranty, contract, tort, or otherwise, whether or not arising out of negligence, and whether or not injury was sustained from, or arose out of the results of, or reliance upon the information.

The display of the DHS official seal or other DHS visual identities, including the US-CERT or ICS-CERT name or logo shall not be interpreted to provide any person or organization the authorization to use the official seal, insignia or other visual identities of the Department of Homeland Security, including US-CERT and ICS-CERT. The DHS seal, insignia, or other visual identities shall not be used in any manner to imply endorsement of any commercial product or activity by DHS, US-CERT, ICS-CERT or the United States Government. Use of the DHS seal without proper authorization violates federal law (e.g., 18 U.S.C. §§ 506, 701, 1017), and is against DHS policies governing usage of its seal.

This presentation is Traffic Light Protocol (TLP): WHITE. Recipients may share TLP: WHITE information without restriction, subject to copyright controls. For more information on the TLP, see http://www.us-cert.gov/tlp.

DHS does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by DHS.

AGENDA

US-CERT IR Lifecycle

US-CERT IRT Services Offered

IRT Trends

Data Breach Trends

IR Best Practices

Common Missteps in IR

Lessons Learned

Mitigation Steps

IRT Background

The US-CERT IRT performs both on-site and remote cybersecurity incident response.

The goal is to discover malicious actors, acquire and analyze malicious tools and activities, and mitigate the intrusion. The IRT is uniquely positioned to assist stakeholders with knowledge of both unclassified and classified actor tactics, techniques, and procedures (TTPs). This position allows IRT to work seamlessly with law enforcement (LE), the intelligence community (IC), and international partners.

IR LiFECYCLE

US-CERT
IRT SERVICES

US-CERT
IRT SERVICES

INCIDENT TRIAGE
Process to scope the severity of an incident and determine what resources are required

NETWORK TOPOLOGY REVIEW
Assessment of network ingress, egress, remote access, segmentation, and interconnectivity with recommendations

INFRASTRUCTURE CONFIGURATION REVIEW
Analysis of core devices on the network that are or can be used for network security. Log Analysis to illuminate possible malicious activity

INCIDENT SPECIFIC RISK OVERVIEW
Provide tailored products and in-person briefings for technical, program manager, or senior leadership audience

CONTINUED

US-CERT IRT SERVICES

HUNT ANALYSIS

Limited deployment of hunt tools to detect indicators of compromise

SECURITY PROGRAM REVIEW

A review of the client's existing security roles, responsibilities, and policies

DIGITAL MEDIA ANALYSIS

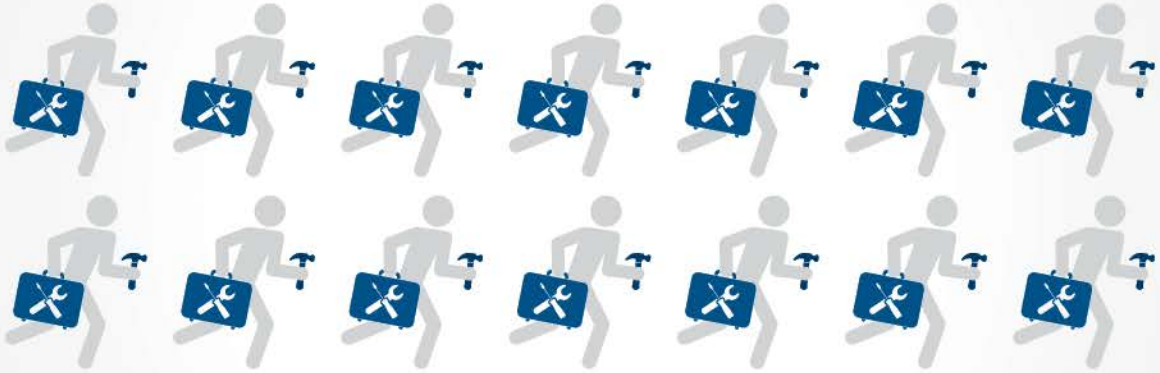
Technical forensic examination of digital artifacts to detect malicious activity and develop further indicators

MALWARE ANALYSIS

Reverse engineering of malware artifacts to determine functionality and build indicators

US-CERT
IRT TRENDS

US-CERT Incident Response Team (IRT) responded to **14** different incidents in 2015.

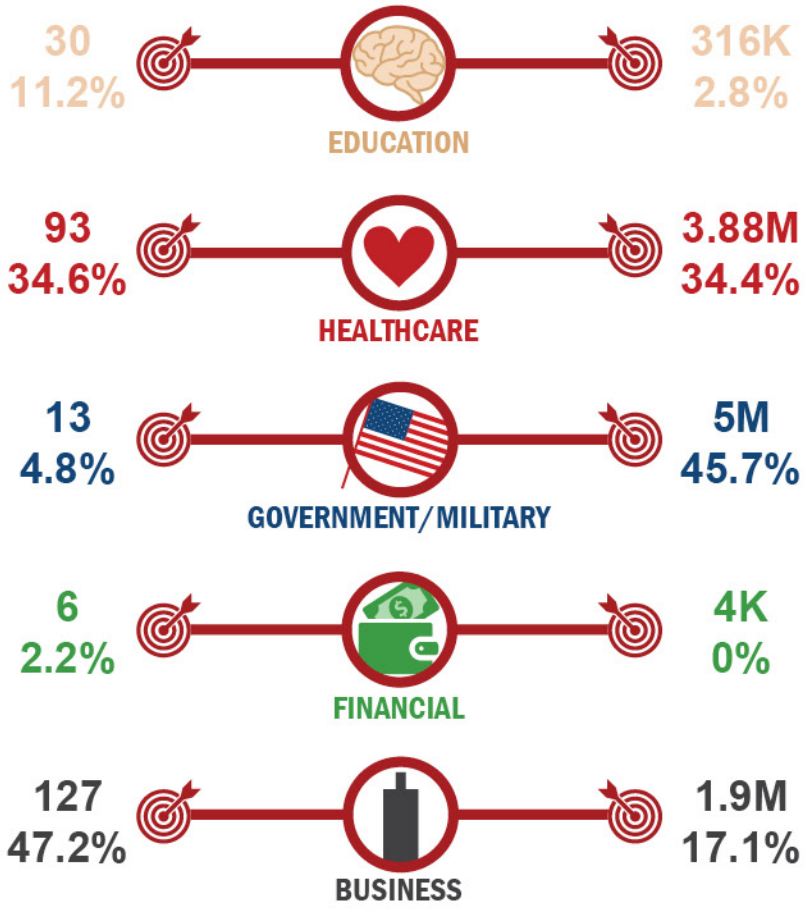


Includes a mix of both government and private sector customers **across the country**

Statistically fewer in number than the 17 engagements from 2014, but **2015 IRT engagements were longer-lasting and larger in scale**

Some of our IRT engagements can last over two months, while **others can be completed in just a weekend or less**

US DATA BREACHES
by Industry: 2016



269

Numbers of Organizations Affected, by Industry Type as of 04/19/2016
(Source: Identity Theft Resource Center)

11.2M

Number/Percentage of Records Breached, by Industry Type 04/19/2016
(Source: Identity Theft Resource Center)

Trends point to bulk PII as a primary target in 2016

IR BEST PRACTICES **PRIOR**

DEVELOP
COMPREHENSIVE INCIDENT RESPONSE PLAN

- Types of incidents
- Assign roles and responsibilities of the response team (and have backups)
- Establish a communication decision tree
- Procedures to follow

EXERCISE
INCIDENT RESPONSE PROCEDURES

- Table Top Exercises
- Simulate forensics scenarios – practice collecting forensic data
- Allows teams to be familiar with tools and be comfortable using them under high-pressure scenarios

IR BEST PRACTICES DURING

INCIDENT IDENTIFICATION

- Fully scope the incident before making any mitigation efforts
- Capture live forensic data and collect logs
- Analyze data to understand lateral movement and persistence mechanisms
- Determine business impact
- Is the adversary still present?

INCIDENT CONTAINMENT

- Closely monitor compromised systems
- Possibly network isolate compromised systems
- Limit scope and magnitude of intrusion
- Gain visibility into the adversary's foothold
  - » Setup alerts for known malicious network infrastructure
  - » Setup alerts for known compromised accounts
  - » Setup alerts for known host-level TTPs
- Create containment & eradication strategy

CONTINUED

IR BEST PRACTICES DURING

INCIDENT ERADICATION

- Remove compromised machines
- Alert/Block known malicious network infrastructure
- Reset user account passwords
- De-privilege user accounts
- Reset service account passwords (difficult!)
- Implement additional controls
- All steps need to be executed in chorus

INCIDENT RECOVERY

- Rebuild compromised hosts offline
- Validate and restore data
- Continue to monitor compromised systems and accounts

IR BEST PRACTICES AFTER

AFTER
THE INCIDENT

- Conduct an after action assessment (lessons learned)
- Identify what worked during the IR process and identify breakdowns or gaps
- Create comprehensive post-incident report
- Revise policies, procedures, IR plans, etc.
- Create new signatures to detect this type of malicious activity
- Identify areas to improve security posture
- Submit incident and recommendations report to leadership

Case Study: OPM

JUNE 2015:

OPM announced that it had once again been the target of a massive data breach potentially affecting millions of Americans.

Initial breach discovered in early 2014 and compromised information about OPM servers, but no PII

This recent breach compromised the PII of approximately 21.5M people, according to the agency

- 19.7M personnel that applied for security clearances
- 1.8M family members

OPM discovered the most recent intrusion on its own using tools that were recommended by US-CERT following the initial intrusion

CONTINUED

Case Study: OPM

Based on guidance provided by US-CERT during mitigation of an earlier cybersecurity incident, the organization began implementing improved cybersecurity capabilities across its networks.

US-CERT substantiated the compromise using EINSTEIN and assessed the potential damage. SMEs from the interagency response team provided guidance in numerous specialized areas such as IBM mainframe and web applications.

US-CERT was provided with digital media for analysis. Analysis of these artifacts led to the identification of the tools used for remote access and lateral movement by the advanced persistent threat (APT) actor.

US-CERT developed indicators of compromise (IOCs) that were shared with trusted partners. IOCs were also used to develop signatures for EINSTEIN.

COMMON MISSTEPS

Common missteps an organization can make when first responding

MITIGATING THE AFFECTED SYSTEMS TOO EARLY

- Can cause the loss of volatile data such as memory and other host based artifacts
- Adversary will notice and change TTPs

TOUCHING ADVERSARY INFRASTRUCTURE (PINGING, NSLOOKUP, BROWSING, ETC)

- These actions can tip off the adversary that they have been detected

PREEMPTIVELY BLOCKING ADVERSARY INFRASTRUCTURE

- Network infrastructure is fairly inexpensive. Adversary can easily change to new C2 and you will lose visibility of their activity.

PREEMPTIVE PASSWORD RESETS

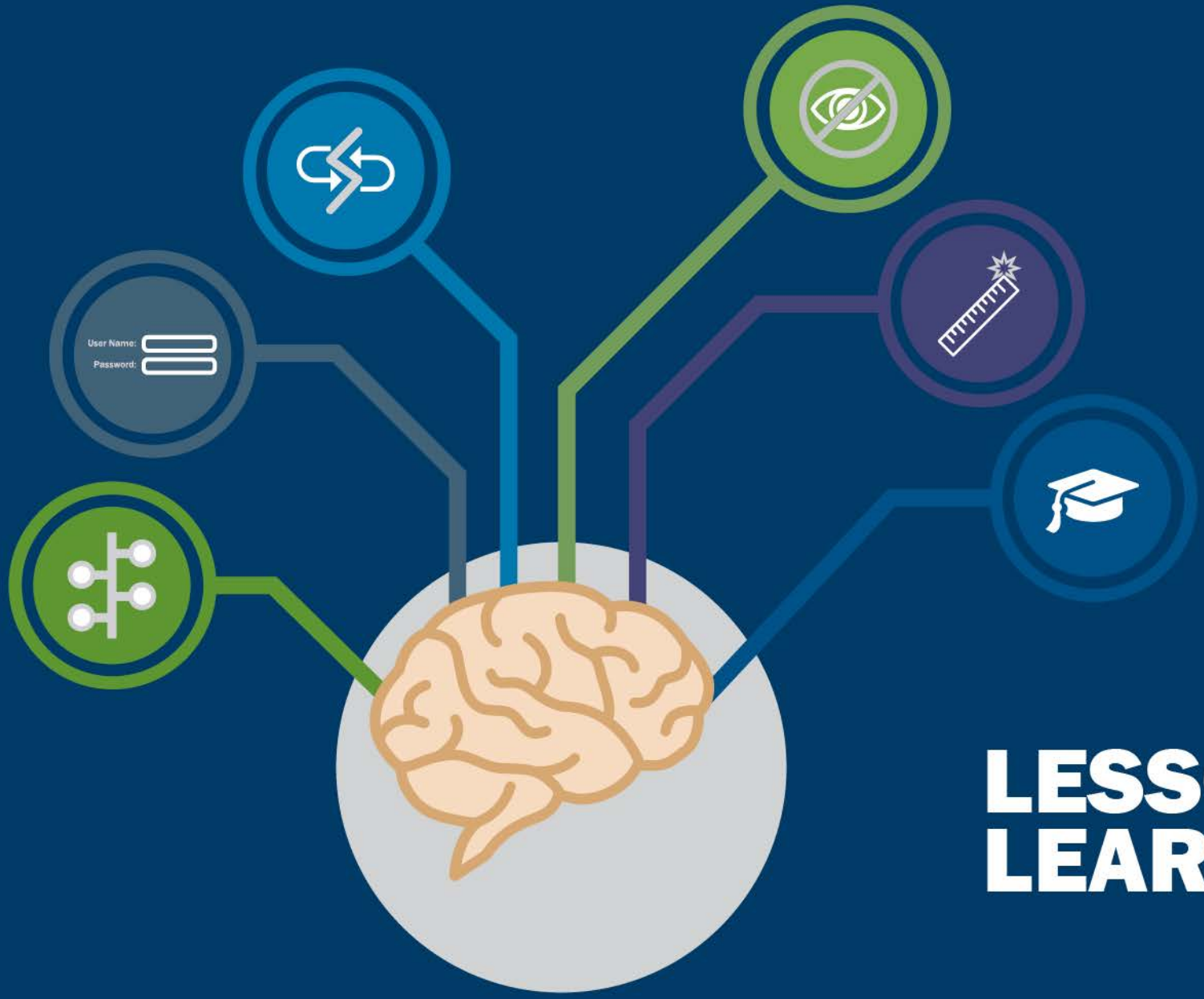
- Adversary likely has multiple credentials – or worse owns your entire AD
- Adversary will use other credentials, create new credentials, or forge tickets

Password

* * * *

FAILURE TO PRESERVE OR COLLECT CRITICAL LOG DATA

- Learn what log types would be critical to an investigation in your organization.
- Collect and retain these logs for at least 1 year.



LESSONS LEARNED

Lessons Learned
Network Segmentation

These cyber events have brought to focus the importance of network segmentation.

- Response teams arrived onsite expecting to assess a defined portion of a corporate network, only to find the network is not segmented from others—which can mean hundreds of sub-networks affected as opposed to just one

- Recommend separating administrative networks from operational networks with physical controls and VLANs

Lessons Learned
General User Accounts are Targets

We are seeing common vulnerabilities exploited and actors compromising general user accounts instead of admin accounts.

- Threat actors can conduct business on the network as an authorized user and elevate privileges as necessary

- Most organizations, all users have access to some sensitive information (fileshares, databases, etc.)

Lessons Learned
Lack of Two-Factor Authentication

- Can minimize attacker moving laterally through network

Lessons Learned
Lack of Network Visibility

- Both retention and verbosity of critical components
- Flow based analysis such as Netflow
- Full Packet Capture for deep packet inspection

Lessons Learned
Poor Server Discipline

- Not hardened or standardized
- Unnecessary web access / programs / services running
- Outdated OS
- Sys admin or leadership reluctant/afraid to change “what’s currently working”

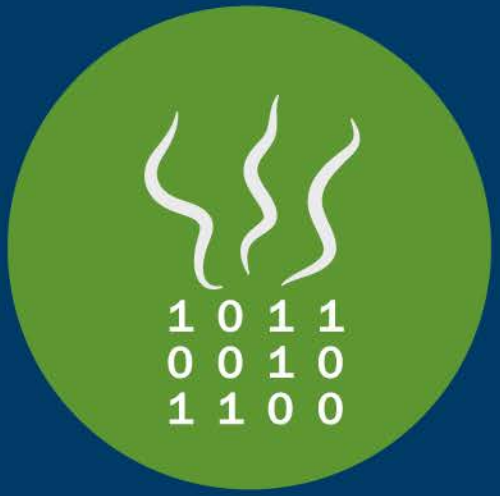
Lessons Learned

Keep Your Workforce Educated

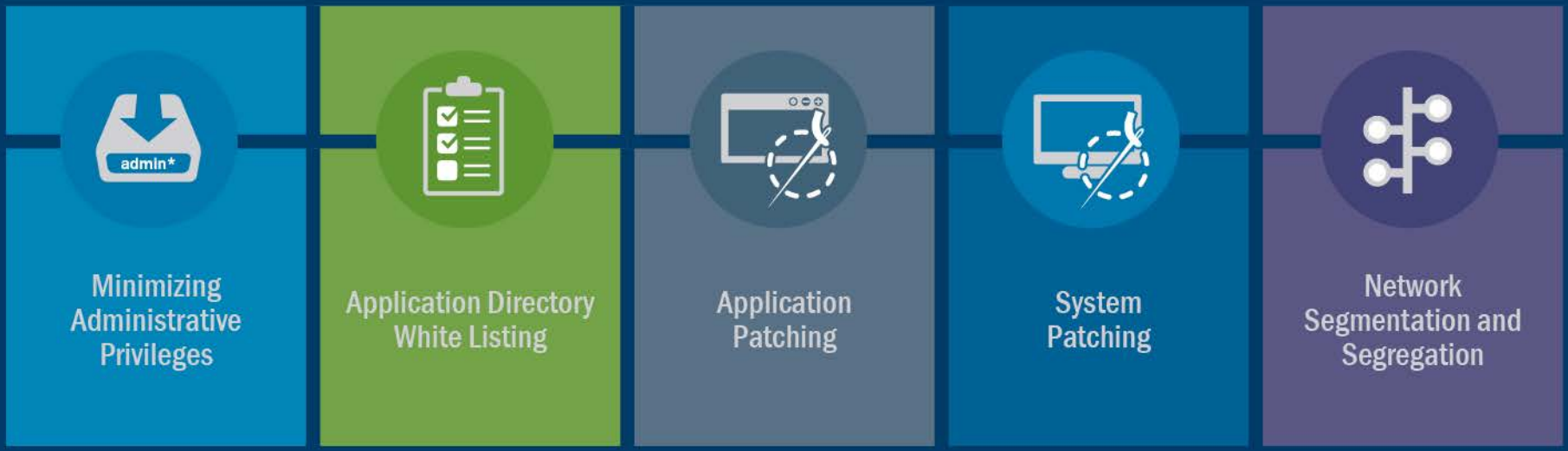
Enhance existing cyber training programs to adapt and transform to evolving cyber environment

- Build cybersecurity awareness and multiple competencies across skilled workforce
- Stay abreast of the cyber threat and the employee's role in security
- Conduct internal phishing tests

MITIGATION
BASIC CYBER HYGIENE
"US-CERT Top 5"



Basic cyber hygiene would prevent approximately 85% of the security breaches security practitioners deal with today.



Questions

CONTACT US-CERT:
info@us-cert.gov
888-282-0870

SUBSCRIBE
to the **National Cyber Awareness System:**
http://www.us-cert.gov/ncas

LEARN
about **US-CERT mailing lists and feeds:**
http://www.us-cert.gov/mailing-lists-and-feeds

FOLLOW
US-CERT on Twitter:
@uscert_gov

REPORT
incidents, **malware**, **phishing**, or **vulnerabilities**:
https://www.us-cert.gov/report

Homeland Security