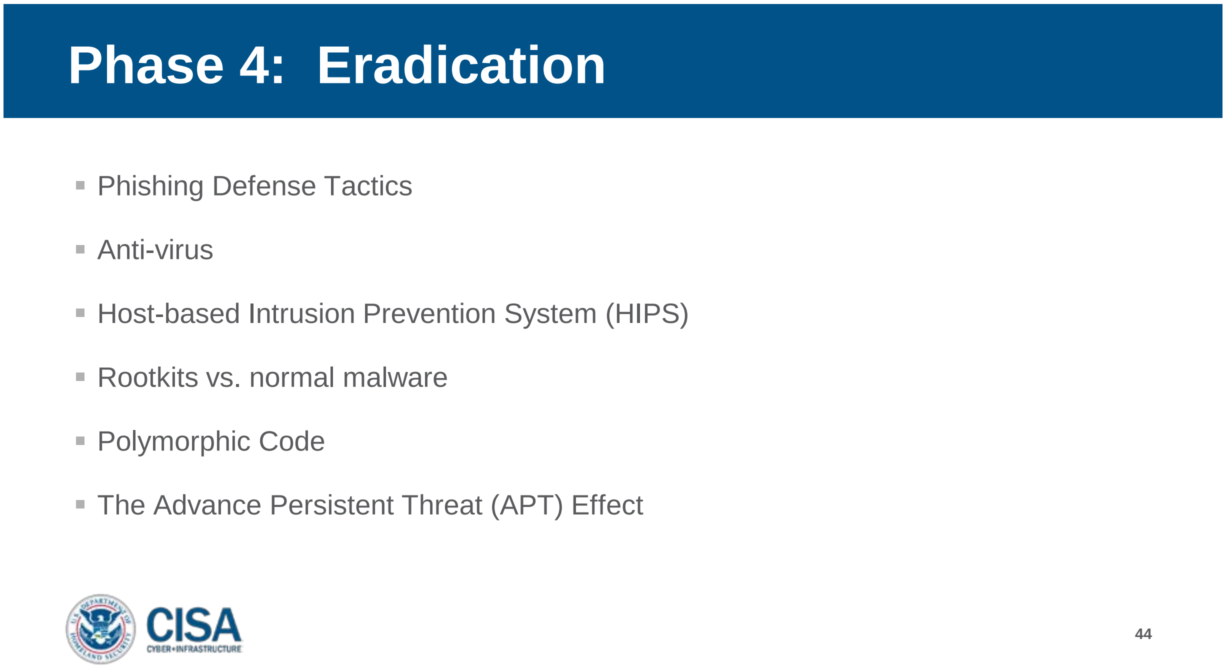
Incident Response Phases 4-5 of 6 – Eradication and Recovery

Table of Contents

Phase 4: Eradication



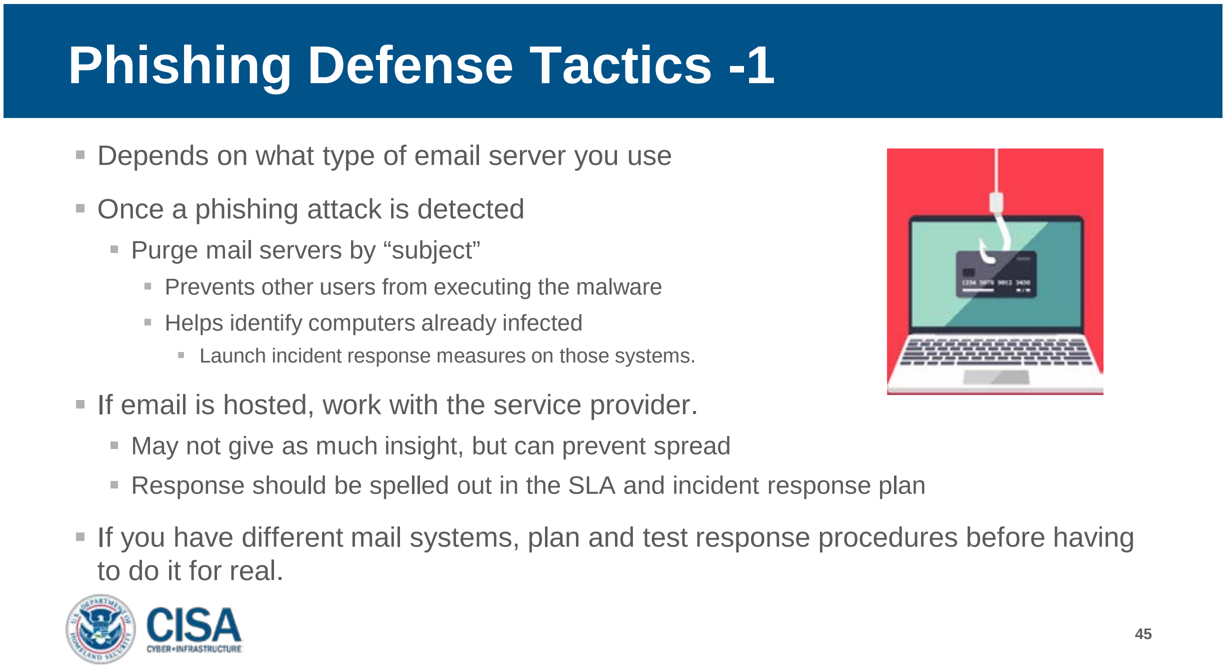
Phase 4: Eradication

- Phishing Defense Tactics
- Anti-virus
- Host-based Intrusion Prevention System (HIPS)
- Rootkits vs. normal malware
- Polymorphic Code
- The Advance Persistent Threat (APT) Effect

CISA
CYBER+INFRASTRUCTURE

**044 Instructor: So, now that we've contained our problem, now we need to eradicate it. And this really boils down to the idea of it's dependent upon the threat. Here are some examples of what we're going to discuss.

Phishing Defense Tactics -1



Phishing Defense Tactics -1

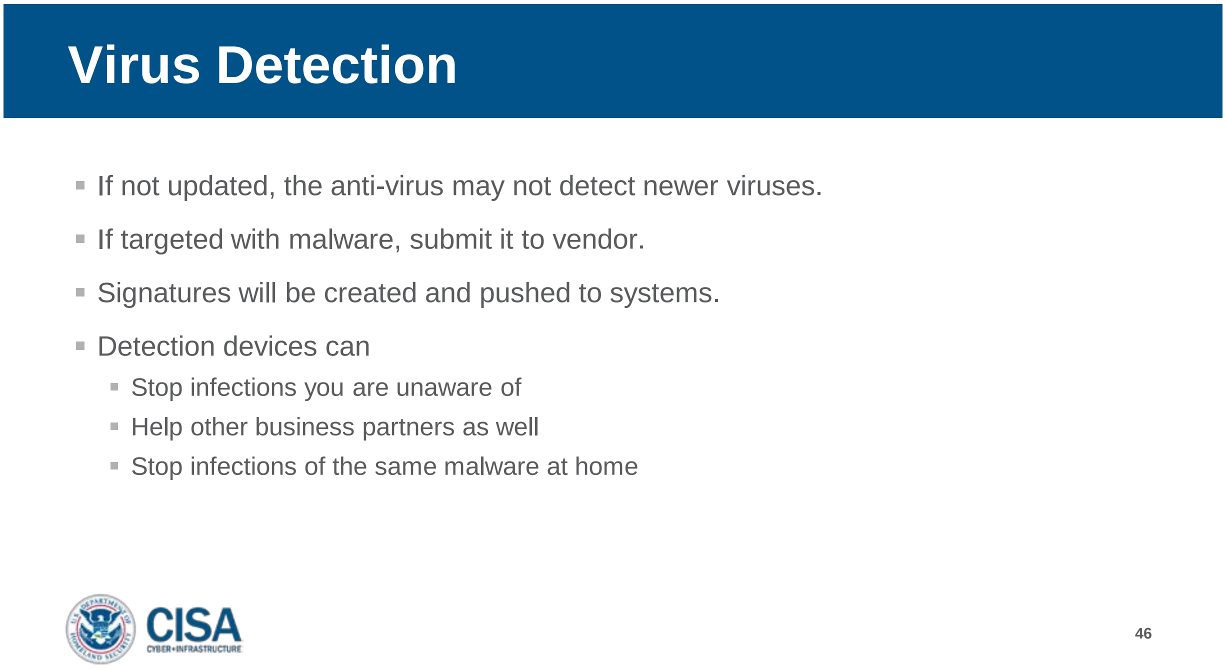
- Depends on what type of email server you use
- Once a phishing attack is detected
  - Purge mail servers by “subject”
    - Prevents other users from executing the malware
    - Helps identify computers already infected
      - Launch incident response measures on those systems.
- If email is hosted, work with the service provider.
  - May not give as much insight, but can prevent spread
  - Response should be spelled out in the SLA and incident response plan
- If you have different mail systems, plan and test response procedures before having to do it for real.

CISA
CYBER+INFRASTRUCTURE

**045 Phishing is a big problem. It's not only a technical problem, it's a social problem as well because you have employees in the enterprise who may not necessarily be educated and may unnecessarily click on every link that they see. It really can depend sometimes too on the email server that you have and that you're using. Clearly, if you have an attack, a known attack that comes in, you can start purging the server of anything that has that common subject line, let's say.

It could also depend if it's a host-based phishing email. Then you want to work with your service provider. It's important to understand here what your service level agreements are with those service providers at this point, so that way you know that their responsibilities are just as much as you know what your responsibilities are.

Virus Detection



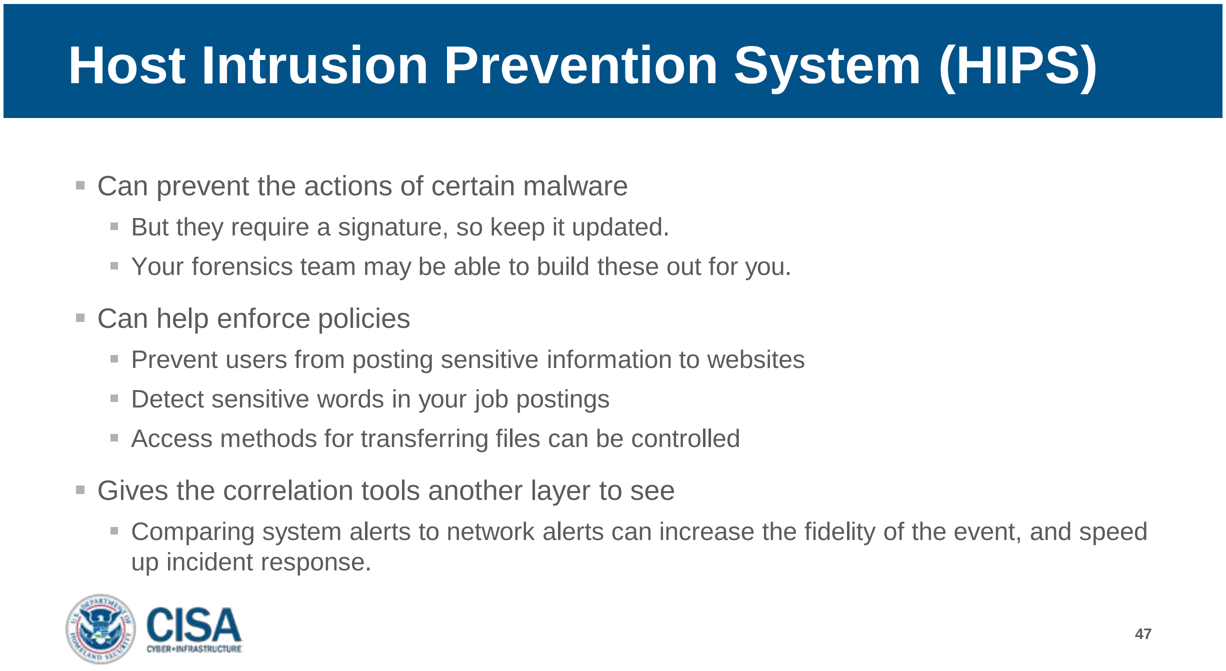
Virus Detection

- If not updated, the anti-virus may not detect newer viruses.
- If targeted with malware, submit it to vendor.
- Signatures will be created and pushed to systems.
- Detection devices can
  - Stop infections you are unaware of
  - Help other business partners as well
  - Stop infections of the same malware at home

CISA
CYBER+INFRASTRUCTURE
46

**046 There's also the issue of antivirus detection. Now, there may be the rare circumstance that you actually identify a new virus out in the wild. If that's the case, be sure to talk to whoever your antivirus vendor might be. There's also other sites like VirusTotal that could help you out in reporting these broadly to the community. If so, new signatures will be assigned to your antivirus software, so that way other systems can identify this virus as it attacks. Basically, what you're trying to do is stop the infection, and you're also going to seek help from other business partners and help them as well to keep yourselves insulated from these infections cropping up.

Host Intrusion Prevention System (HIPS)



Host Intrusion Prevention System (HIPS)

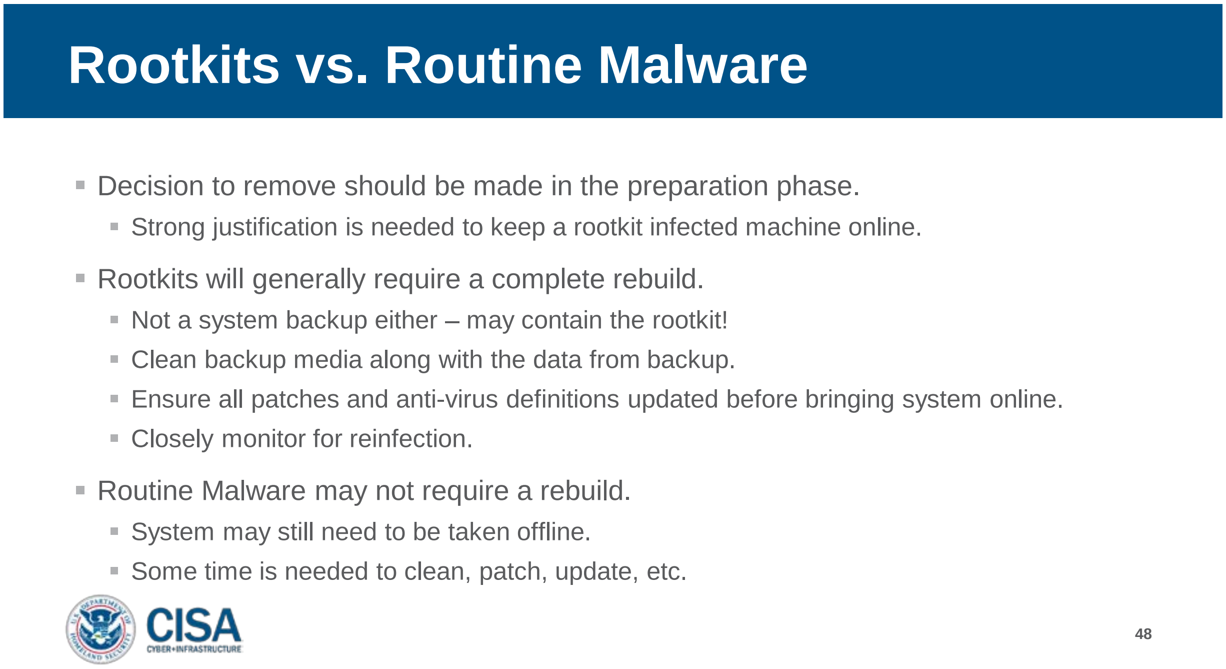
- Can prevent the actions of certain malware
  - But they require a signature, so keep it updated.
  - Your forensics team may be able to build these out for you.
- Can help enforce policies
  - Prevent users from posting sensitive information to websites
  - Detect sensitive words in your job postings
  - Access methods for transferring files can be controlled
- Gives the correlation tools another layer to see
  - Comparing system alerts to network alerts can increase the fidelity of the event, and speed up incident response.

47

**047 You can also have a host intrusion prevention system, commonly called HIPS. Now, what we really want to do here is we want to prevent malware from getting in our system. It's also signature based. So, it's good to keep in mind that the system needs to be updated from time to time. And it's really going to help you enforce policies that you have based around your system. For example, suppose you have policies against posting certain sensitive information to certain websites. It kind of acts like a data loss prevention tool in that regard. It makes sure that you're not bleeding out information. Now, this is really where it helps too in that you could leverage your classification system, so it can help in that regard as well.

The other thing that HIPS may help with is it actually provides a correlation tool, so that way you can actually see what traffic is coming in and compare it to previous traffic, so that way you know if you have a trend of a negative event that's cropping up.

Rootkits vs. Routine Malware

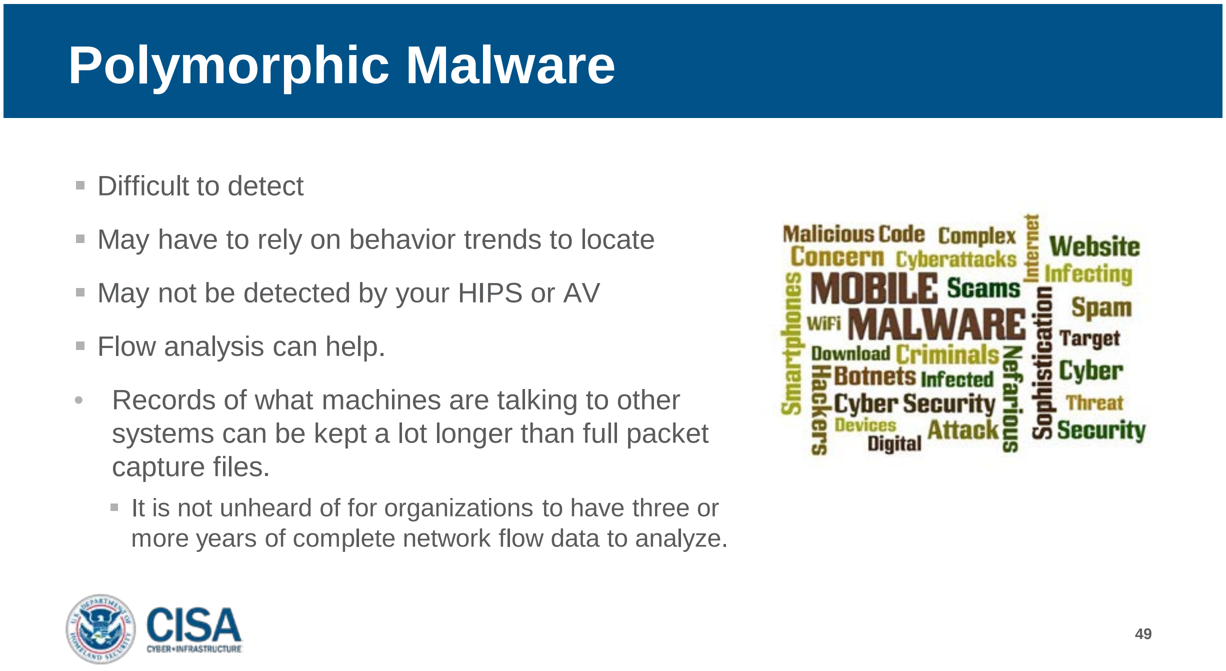


Rootkits vs. Routine Malware

- Decision to remove should be made in the preparation phase.
  - Strong justification is needed to keep a rootkit infected machine online.
- Rootkits will generally require a complete rebuild.
  - Not a system backup either – may contain the rootkit!
  - Clean backup media along with the data from backup.
  - Ensure all patches and anti-virus definitions updated before bringing system online.
  - Closely monitor for reinfection.
- Routine Malware may not require a rebuild.
  - System may still need to be taken offline.
  - Some time is needed to clean, patch, update, etc.

**048 Rootkits can be particularly pernicious. You've got to be really careful with this. The idea here is that you have something that's penetrated your system and is actually down in the software such that you would actually have to rebuild your entire system to get rid of it. Be mindful of the idea that this is a critical business decision, and it could have significant interruption that comes along with it.

Polymorphic Malware



Polymorphic Malware

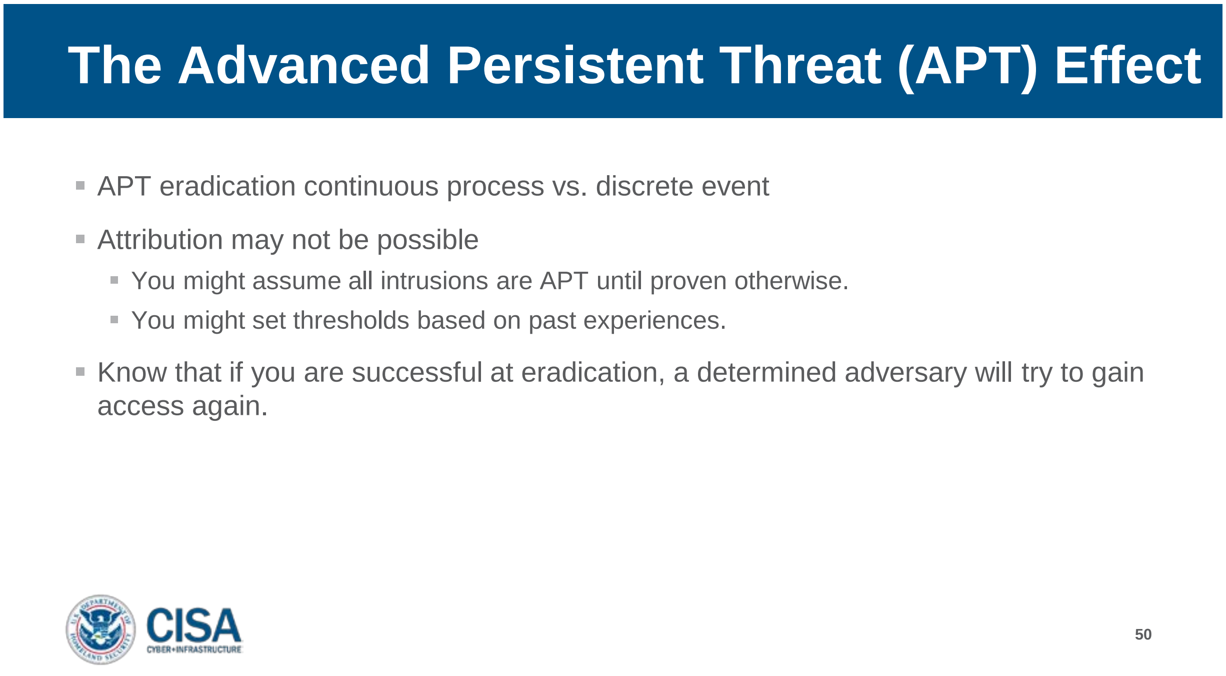
- Difficult to detect
- May have to rely on behavior trends to locate
- May not be detected by your HIPS or AV
- Flow analysis can help.
- Records of what machines are talking to other systems can be kept a lot longer than full packet capture files.
  - It is not unheard of for organizations to have three or more years of complete network flow data to analyze.

Malicious Code
Complex
Internet
Website
Concern
Cyberattacks
Infecting
Smartphones
MOBILE
Scams
Spam
WiFi
MALWARE
Sophistication
Target
Download
Criminals
Nefarious
Cyber
Hackers
Botnets
Infected
Cyber Security
Threat
Devices
Digital
Attack
Security
CISA
CYBER+INFRASTRUCTURE

49

**049 Some malware will change over time. It could be polymorphic, and it's going to be incredibly difficult to detect. So, what you want to do is you want to make sure, once again, that your HIPS and your antivirus software is up to date as best as possible. And at times, what you could do is you could use flow analysis of the data that's coming into your system and going out, so that way you can understand if you have something in their system that's providing a trend that you have something bad going on. It's not unheard of really to have three or four years of data resident on your system so that you can continue to conduct this analysis.

The Advanced Persistent Threat (APT) Effect



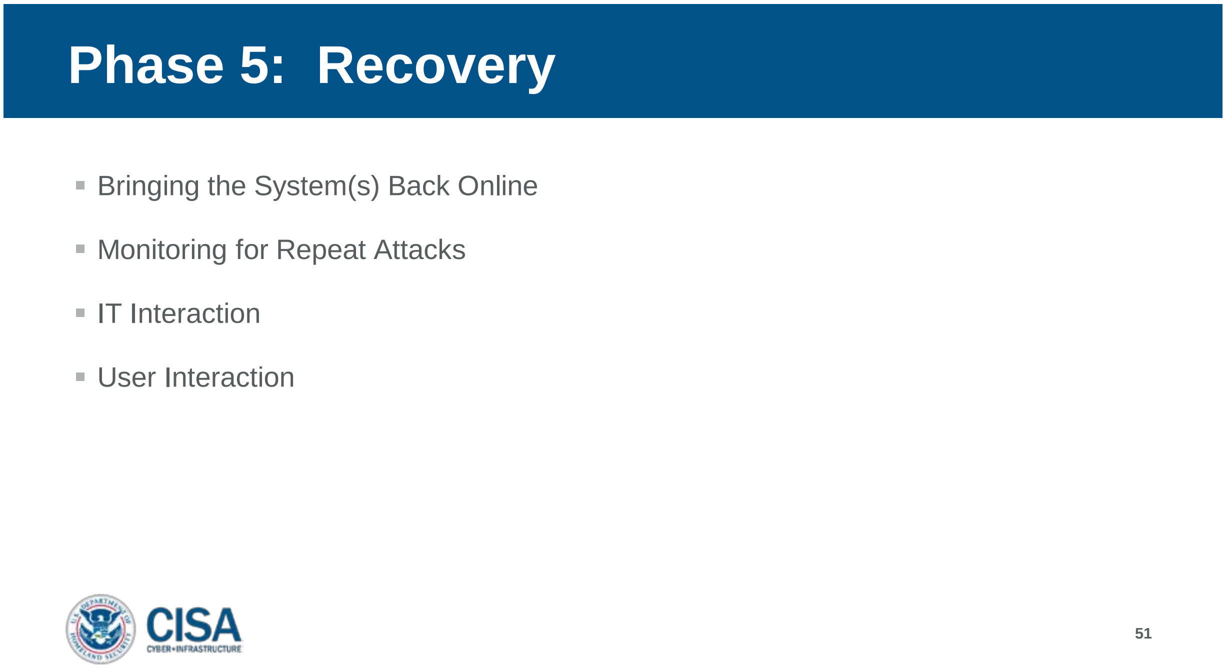
The Advanced Persistent Threat (APT) Effect

- APT eradication continuous process vs. discrete event
- Attribution may not be possible
  - You might assume all intrusions are APT until proven otherwise.
  - You might set thresholds based on past experiences.
- Know that if you are successful at eradication, a determined adversary will try to gain access again.

50

**050 We also have this notion of having somebody who gets into your system and is truly like a low, slow flier. They get in there, and, to be honest, they're hiding resident in the system, and they're really in the weeds and really hard to pick up any trends of anything that they're doing. So, these are called advanced persistent threats. It's hard to get rid of them. It's hard to even identify them. So, really what you want to do is have a continuous process for monitoring to make sure that you can see any unusual trends that are occurring on your system, especially over long periods of time. Please note, that even if you do find an APT, or any of these viruses, for that matter, that if you do not patch your system or change the vulnerability, or update to correct the vulnerability you had in your system, they will likely try again, and they will be successful.

Phase 5: Recovery



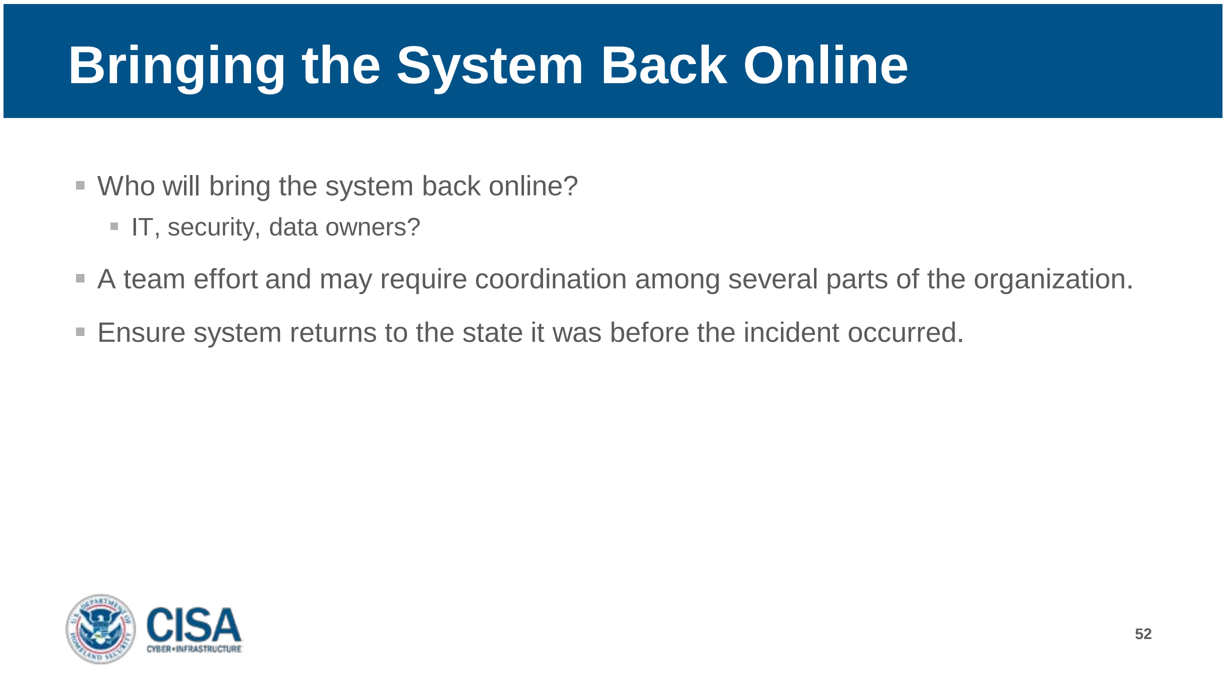
Phase 5: Recovery

- Bringing the System(s) Back Online
- Monitoring for Repeat Attacks
- IT Interaction
- User Interaction

51

**051 Okay so, now that we've eradicated the problem, we need to recover our system. We need to bring it back to life. We need to get our organization back on its feet again. There's a couple things you have to think about as you do that.

Bringing the System Back Online



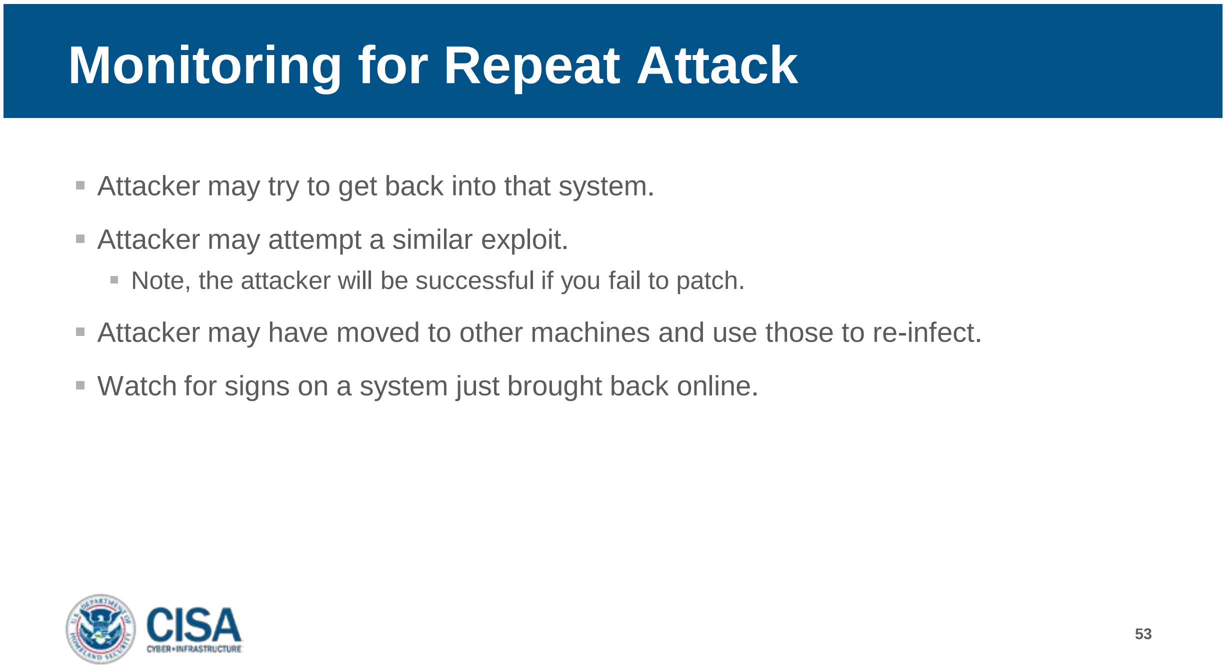
Bringing the System Back Online

- Who will bring the system back online?
  - IT, security, data owners?
- A team effort and may require coordination among several parts of the organization.
- Ensure system returns to the state it was before the incident occurred.

52

**052 First of all, actually bringing a system online can be trickier than you think. It's more than just hitting a power button at times. It depends on the complexity of your network and how things work together. Be mindful of the idea that just as a security organization, you may need to interface with the IT organization, data owners, and others in your organization to coordinate this start up.

Monitoring for Repeat Attack



Monitoring for Repeat Attack

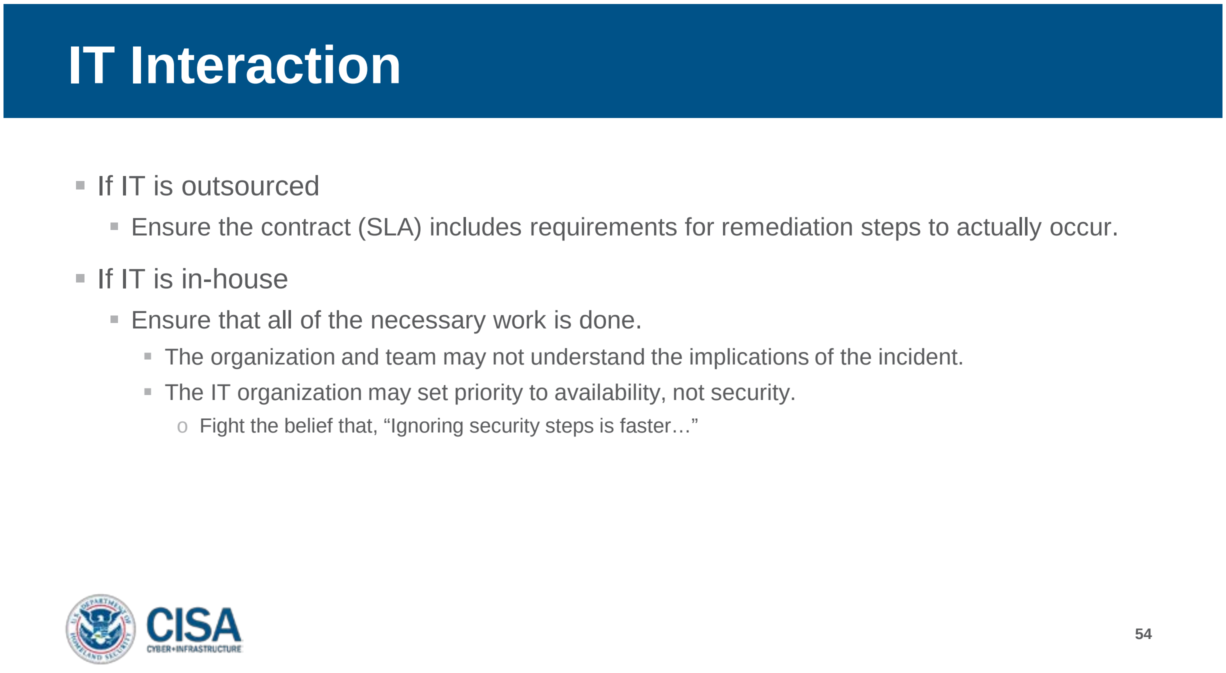
- Attacker may try to get back into that system.
- Attacker may attempt a similar exploit.
  - Note, the attacker will be successful if you fail to patch.
- Attacker may have moved to other machines and use those to re-infect.
- Watch for signs on a system just brought back online.

CISA
CYBER+INFRASTRUCTURE

53

**053 Once you do have it started up, you really need to make sure that you don't have a higher likelihood of a repeat attack. Remember, you have to keep your system up to date, and you have to correct the vulnerability that had taken place the first time that allowed the initial attack to be successful. And then you're going to watch for existing trends to see if you have that same exploit still operating on your system. Just as you bring the system online, this is typically where you might see the trend starting immediately after. So, it's a good idea to keep watch immediately after you've brought the system back up and for a period thereafter.

IT Interaction



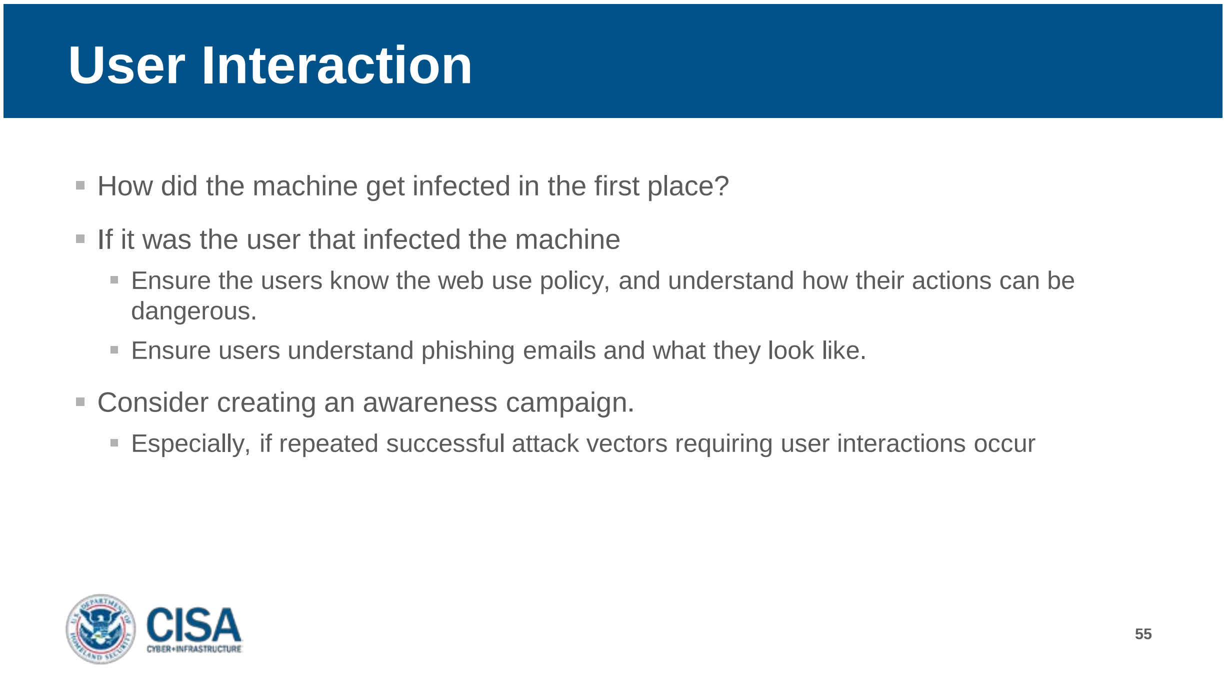
IT Interaction

- If IT is outsourced
  - Ensure the contract (SLA) includes requirements for remediation steps to actually occur.
- If IT is in-house
  - Ensure that all of the necessary work is done.
    - The organization and team may not understand the implications of the incident.
    - The IT organization may set priority to availability, not security.
      - Fight the belief that, “Ignoring security steps is faster…”

54

**054 Also, you need to be mindful of how you're interacting with your IT organization. Once again, you're acting as a team. Now, the trick here is if you have IT outsourced in your organization. If you have service level agreements, you need to be very clear as to whose responsibility is what in the circumstance where these incidents take place. If your IT is in house, you need to have a clear understanding of division of labor and who is responsible for who takes what actions, so that way nothing gets missed.

User Interaction

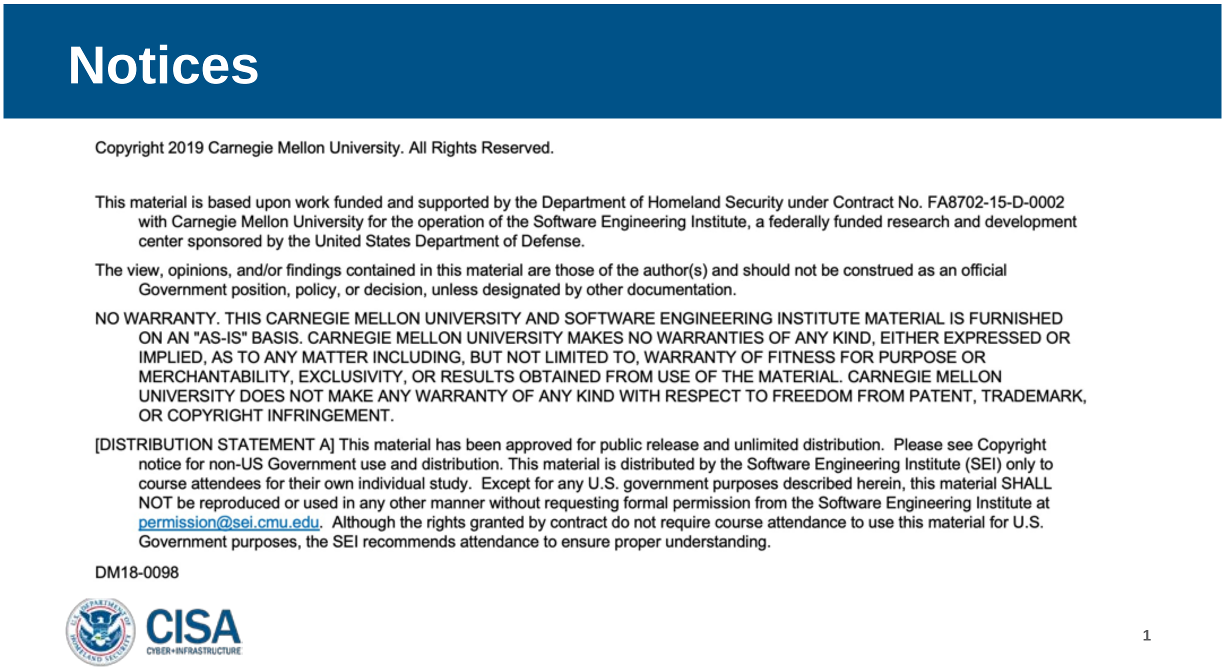


User Interaction

- How did the machine get infected in the first place?
- If it was the user that infected the machine
  - Ensure the users know the web use policy, and understand how their actions can be dangerous.
  - Ensure users understand phishing emails and what they look like.
- Consider creating an awareness campaign.
  - Especially, if repeated successful attack vectors requiring user interactions occur

**055 You also have to have a clear interaction with your users, and this may come down to actually communicating with them in a clear and consistent manner. First of all, it's going to come down to understanding how the system got infected in the first place. You may be even able to narrow it down to a specific user who maybe made the mistake. Remember, it could be an error of ignorance. It could be something as easy as they opened up an email with some kind of bad link in it. So, you have to make sure whoever these users were that they are very much aware of the existing policy. Take it as a learning opportunity. Trust me, the carrot works better than the stick at times. Make sure everybody stays educated, so that way you have a better overall insulated enterprise.

Notices



Notices

This material is based upon work funded and supported by the Department of Homeland Security 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 sponsored by the United States Department of Defense.

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.

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.

DM18-0098