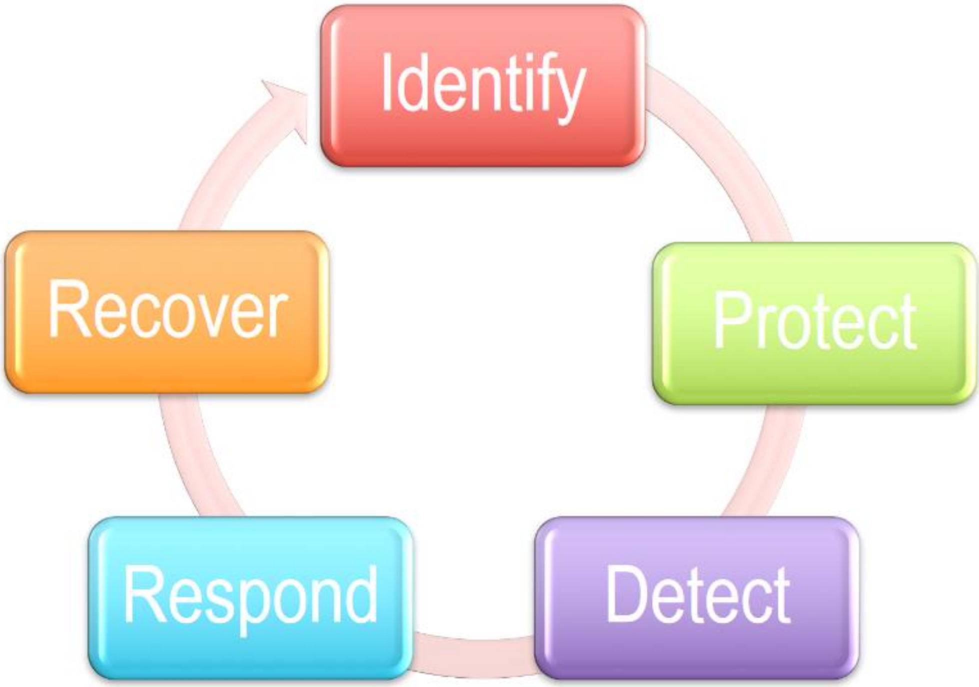
This pamphlet aims to provide a simple, widely applicable overview of how an organization can effectively respond to a cybersecurity event. Because it is only one component of a project centered on the development of a keylogger, this guide finds its greatest utility when used to inform responses to this particular type of malware. However, because many of the broader principles of cyber security response are applicable across a number of event types, we expect that the frequent reference to keyloggers will not detract from this pamphlet's wider applicability. Instead, knowing that specific examples often help to demonstrate general principles, we intend that this pamphlet prove useful across a range of potential threats, regardless of its position in a keylogger-based project.



What is a Keylogger?

A keylogger is a type of malware capable of surreptitiously creating a log of the keys pressed on a machine. Although such a log may have licit uses, a keylogger is also a potent tool for a cyber attacker. There are multiple types of keyloggers with multiple applications, including both hardware and software keyloggers. Software keyloggers can be difficult to detect for antivirus software and firewalls, which makes them especially threatening once they infect a machine. Many modern keyloggers have multiple functions besides recording a victim’s keystrokes: some can also take screenshots and record audio from a connected microphone.

Malicious keyloggers install themselves on a machine when a victim unknowingly opens an infected file, which often arrives through a phishing attempt or other forms of social engineering. Most keyloggers come in a package, usually a deceitful app or file (sometimes known as a Trojan). Because other malicious software may have come bundled along with the keylogger, it is important that when a keylogger is identified on a system the infected machine is also scanned for other malicious software.

Types of assets a keylogger threatens:

1. Passwords
2. Pin numbers
3. User names
4. Email addresses
5. Account numbers
6. Browser histories
7. Workflows
8. Data entry

If you can type it, a keylogger can record it. It is difficult to overstate the damage that an undetected keylogger might do to an otherwise secure network.

5 Types of Keyloggers to Watch For:

1. API-Based Keyloggers: Keyloggers that use keyboard API (application programming interface) to record keystrokes. These keyloggers intercept the notification sent by the keyboard to an application and logs the captured data in a file kept somewhere on the machine.

2. Form Grabbing-Based Keyloggers: Keyloggers that log data from web forms upon submission. These keyloggers intercept the submission notification and log all information provided in the form. The process is completed before the form is submitted to the intended website.

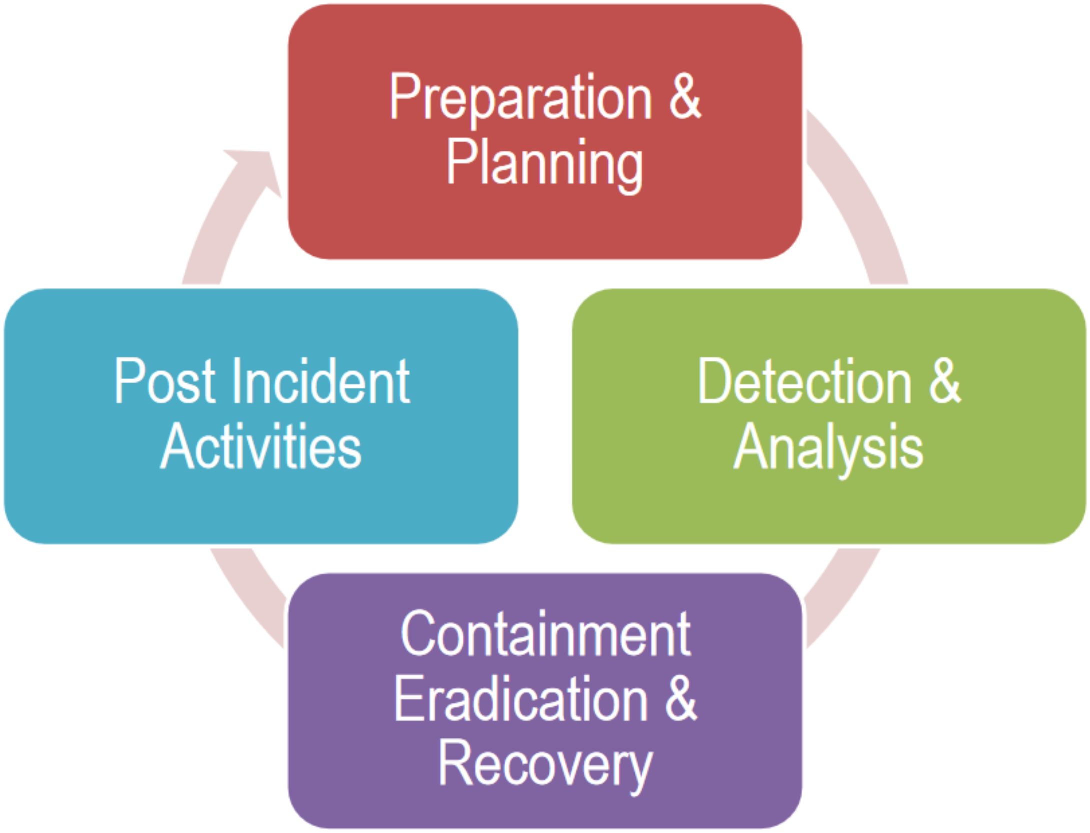
3. Kernel-Based Keyloggers: Keyloggers that hide inside the OS and record keystrokes as they interact with the kernel. Difficult to detect and remove, these keyloggers tend to be distributed by rootkits.

4. Hardware Keyloggers: Keylogging devices that use the circuitry inside a keyboard to log keystrokes. This type of keylogger tends to come built into the keyboard itself, but can also come as a USB connector or mini-PCI card. All records of this type are kept in the internal memory of the malicious hardware.

5. Acoustic Keyloggers: Keyloggers that use cryptanalysis to record keystrokes on the hardware level. These types of keyloggers are rarely used due to their complexity and reduced accuracy compared to other keylogger types.

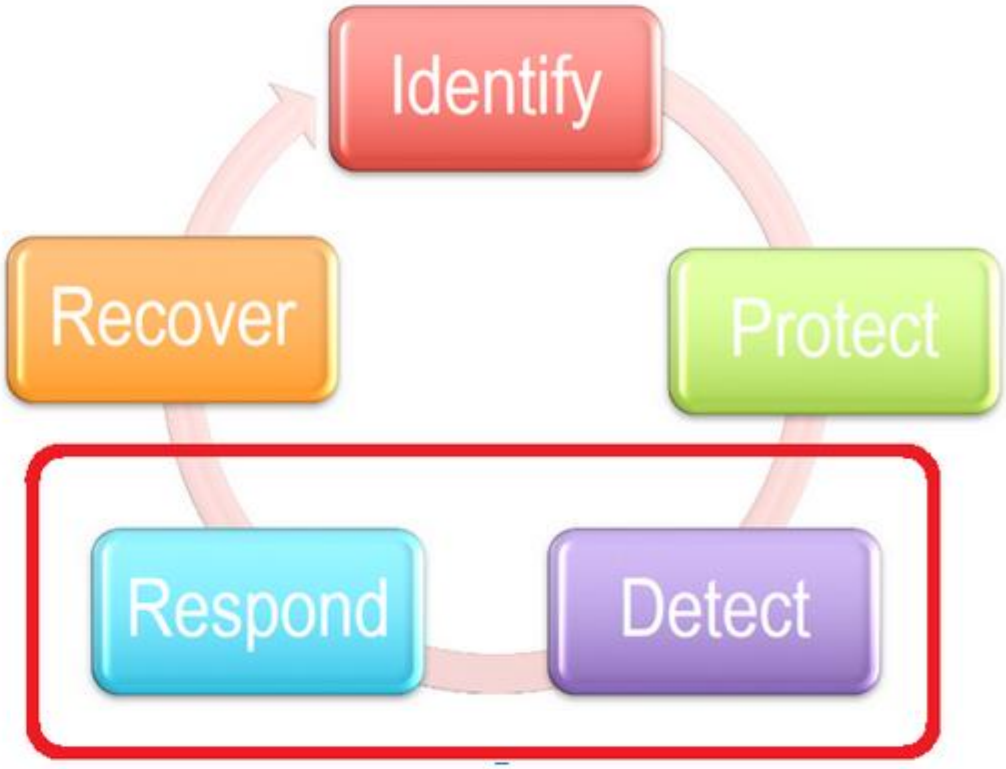
How do we detect keyloggers on our systems?

- Up-to-date antivirus and malware protection
- Monitor and log resource allocation and process usage
  - Helps cybersec team notice anomalies. Anomalies like keyloggers



Let’s assume our organization’s SIEM tools or antivirus software successfully detect the software keylogger we presented. Given this state of affairs:

A. Where are we in the NIST framework?
    a. Detect => Respond



B. Because we implement effective cybersecurity practices, we have a head start on the following
   a. Already know what systems we are responsible for protecting
   b. Know which services are central to the enterprise's functioning
   c. Our response team understands their roles and responsibilities

C. Steps to Take:
   1. Assemble response team
   2. Detect the source/type of incident (in this case, keylogger)
   3. Contain and recover
   4. Assess damage and severity
   5. Begin notification process
   6. Assemble lessons learned

Because this guide focuses on responding to a specific type of malware, our remediation steps will chiefly address topics 2-4, above: Detection, containment, damage assessment.

Detection & Analysis

Detect the source/type of incident:

The keylogger in question requires three key abilities in order to function properly, and each one provides a potential avenue for detection. These processes are: the execution of a malicious script, the creation of a file where keylogs are stored, and the export of these keylog files.

Proper **logging** of all events on our network allows us to detect one or ideally both of these processes.

Even if a user were to download, access, or otherwise install a file containing a malicious script, our organization's proper use of SIEM tools would allow analysts from our SOC to detect the execution of a key logging script. SIEM tools allow SOC analysts to monitor all processes that are occurring on our systems, providing them an opportunity to intervene on a non-authorized process, in this case the keylogger.

Employment of up-to-date **antivirus and anti-malware programs** should provide our network protection against this keylogger, and might detect more than one of its functions. Security programs can detect known keyloggers by hashing, and more sophisticated anti-malware tools may detect keylogger-like behaviour via heuristic analysis. Keyloggers are often packaged along with other types of malware, or inserted as part of another malware package, for instance a Trojan. Antivirus and antimalware programs' ability to detect and defeat such threats make them a potent tool in combating keyloggers.

Finally, proper logging of incoming and outbound connections could provide an opportunity for detecting a software keylogger. The sample keylogger we have displayed here generates a file full of logged keystrokes that a malicious attacker needs to access—otherwise the data simply remains on our system. One method of extracting this information would be to connect to our networks at a specific time from a particular origin point. **Noticing an unauthorized, outbound connection** is a key competency for our SOC, and provides a method of detecting this attack.

Containment Eradication & Recovery

Contain and Recover:

Containing and recovering from a keylogger attack will require us to do two things:

1) Identify what systems, networks and assets have been compromised
2) Determine what information has been disclosed to unauthorised parties.

Having already detected the malware in question, our response team should now generate a working understanding of what the malware is, how it works, and what can be done to look for it across our entire network. In order to properly contain the threat, members of our cyber response team must create a widely applicable understanding of what the threat is. They should:

1) Develop a profile of the malware program
2) Understand what permissions the program requires in order for users to execute it
3) Catalogue which locations/directories/filepaths the malware resides in

Effective containment and eradication builds upon these three efforts. For reference, in the case of the keylogger we generated for this demonstration, a profile of the malware program would note that the keylogger executes a specific script and creates a log file with specific naming attributes. These aspects of the program would provide clues for the response team to follow in isolating or eliminating the malware.

Once our response team has a comprehensive understanding of which network components this malware has compromised, the next task is to determine what information this keylogger might have extracted. As noted above, keyloggers can execute a number of functions beyond simply logging keystrokes. The malware in question, however, only logs keystrokes, indicating a potentially simpler path to recovery. If our response team knows they are only responsible for identifying potential leaks of keystrokes, they can triage their efforts accordingly.

Having determined which systems the keylogger infected, as per the above, responders can pinpoint which data might potentially have been leaked by the presence of this keylogger.

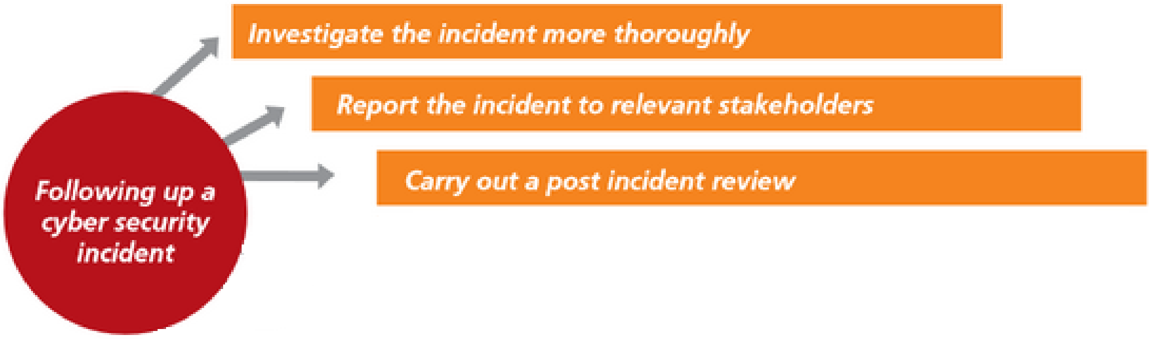
Post Incident Activities

Damage Assessment, Communication:

______Post-incident activities will chiefly focus on two areas, assessing damage and communicating the compromise to relevant stakeholders.

Our damage assessment should have the immediate goal of determining the extent of damage to our network and quantifying the business impact of malicious activity. Once a detailed picture of damage to our network is generated, we will have a general sense of what reporting requirements we have.

Reporting requirements include fulfilling our duties to customers and business partners, but also include a critical legal component. Specific federal and local guidelines may place a further reporting burden on our organization. Remaining aware of and responding to legal requirements is a cyber security must.


Following up a cyber security incident
Investigate the incident more thoroughly
Report the incident to relevant stakeholders
Carry out a post incident review