Bitdefender®

Endpoint Detection and Response

Key instrument for Security Incident Response

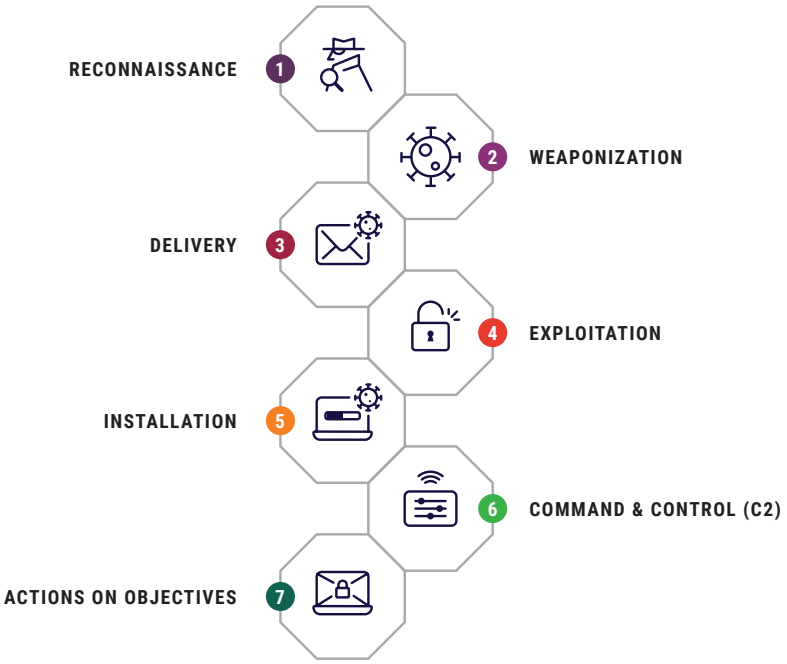
Summary

The birth of a data breach

Personal data records belonging to more than 4 billion people were affected by the top 10 data breaches alone in the last decade[1]. Businesses are losing market capitalization, reputation and customers, besides costly legal consequences once these data breaches surface. And, statistics indicate cybercrime is here to stay and thrive. As business dependency on IT grows, so does cyber criminals' interest in taking advantage of this trend. So, what can be done? How can enterprises around the globe effectively fight cybercrime and prevent costly data breaches?

Data exfiltration or destruction, IT service unavailability and performance drops due to cryptojacking are only the last stage of a much longer and normally complex chain of events, known as the attack kill-chain.

The attack kill-chain is a sequence of actions an attacker follows in preparing and executing an attack. Most attacks, especially advanced attacks, go through several phases:



1. Reconnaissance: Intruder selects target, researches it, and attempts to identify vulnerabilities in the target infrastructure.

2. Weaponization: Intruder creates (or finds on the exploit databases) remote access malware weapon, such as an exploit, virus or worm, tailored for one or more vulnerabilities.

3. Delivery: Intruder transmits weapon to target (e.g., via e-mail attachments, websites or USB drives)

4. Exploitation: Malware weapon's program acts against target endpoint to exploit vulnerability.

5. Installation: Malware weapon installs access tools (e.g., "backdoor") usable by the attacker.

6. Command and Control: Malware enables intruder to gain persistent access to target infrastructure.

7. Actions on Objective: Intruder takes action to achieve goals, such as data exfiltration, data destruction, or encryption for ransom.

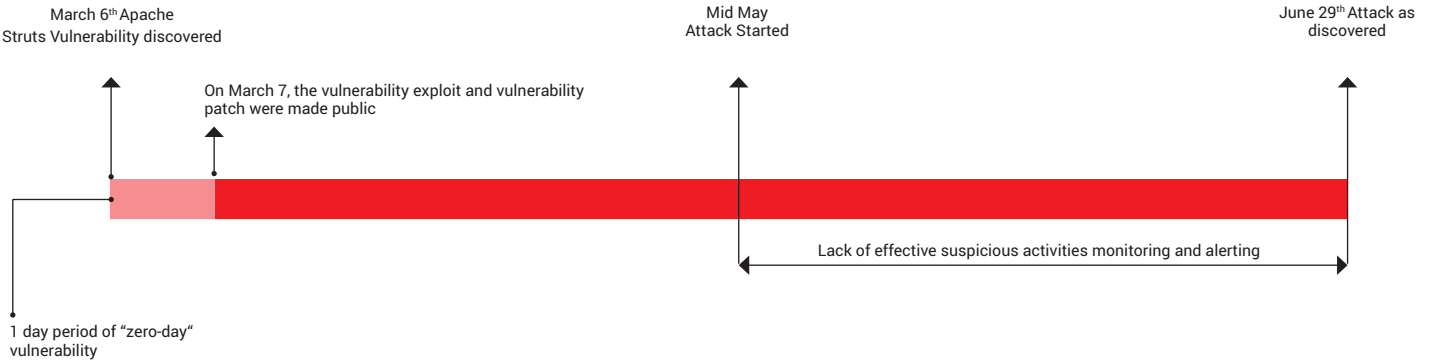
Any of the actions described above may leave traces which, once discovered by enterprise security teams, raise a security incident. Undetected, ignored or unmanaged security incidents eventually lead to data breaches.

Assume breach mentality

No matter how serious an organization takes cybersecurity, it's impossible to prevent all incidents or breaches. Identifying incidents early in the attack kill-chain and being prepared to respond to them makes the difference between a breach with minor losses and one with severe consequences for the enterprise. The 2017 Equifax scandal illustrates the need for proper incident identification instruments and incident response plans.

The chain of events started with an Apache Struts vulnerability[2] discovered on March 6th. Apache Struts 2 is an open-source web application framework for developing Java web applications. The Apache Struts 2 users were warned in March of "possible [remote code execution] when performing file upload…." Remote code execution exploit associated with Struts allowed attackers to take over a server via malicious code.

On March 7, the vulnerability exploit and vulnerability patch were made public[3], leaving a "zero-day vulnerability" window of only one day. Based on later investigations, it seems the attack on the unpatched Equifax systems started in mid-May, 2.5 months after the vulnerability patch was released. This is not uncommon, as statistics show that many enterprises are more than 30 days behind with security patching.



From mid-May to July 29th, when the breach was discovered by Equifax staff, 143 million data records were exfiltrated. Almost 3 months passed with little or no warning as to what was going on. Besides the other security issues that were entirely avoidable, there was no effective mechanisms to raise alerts regarding suspicious activities in the IT infrastructure. The end of the story could have been significantly different and the damages far less costly if incident management plans and instruments were in place and the attack had been discovered early.

Managing security incidents effectively

Understanding the attack kill-chain is important, but applying a methodical approach to incident management is equally important. Similar to an attack kill-chain, the incident response plan is a sequence of steps: Prepare, Identify, Contain, Eradicate, Recover and Learn.

Each step has specific objectives. When attacks occur, the security team (or incident response team) must be prepared and act with precision. To effectively manage security incidents an organization must employ 3 categories of resources: People, Processes and Tools. The objective of the prepare phase is to prepare security teams, create policies, processes and select tools that can help prevent, detect and respond to incidents to minimize the consequences of the attack.

During the Identify phase, the incident response teams must clearly determine if an event, or sequence of events, is an information security incident and what are the likely consequences.

Once an attack affecting personal data records is identified, the immediate action is to contain the attack. This means identifying the affected systems, stopping the ongoing attack and, also important, preventing the attack from spreading to other endpoints in the infrastructure.

Once the attack has stopped, the security teams can focus on eliminating the malware, deleting any artifacts left by malicious software and restoring pre-attack configuration of endpoints.

The objective of the recovery phase is to fully restore the compromised assets to achieve full operational status. For example, the case of a corrupt database containing Personal Data records would mean restoring the database from backups.

People and Processes – key elements of Incident Response Strategy

Organizations tend to spend a great deal of attention into selecting the best tools for incident response but equal effort must be dedicated to developing the teams and processes. For effective incident response, incident analysis or threat hunting as a fulltime job responsibility works best and developing teams with threat hunting capabilities should be on top of CISO priority lists.

There are multiple models and approaches for developing a security architecture and an incident response process. One of the best available is the model provided by Gartner, named CARTA[4] – continuous adaptive risk and trust assessment. It is a comprehensive framework detailing how modern tactics, technologies and tools can be used to counter cyber-attacks. It details the 4 main elements of the recommended Security Architecture: Prevent, Detect, Respond and Predict. Each element consists of other smaller components.

Figure: High-level Security Architecture

For example, the Detection phase (one of the most important for incident response) consists of:
- Detect incidents
- Confirm and prioritize risk
- Contain incidents

Respond phase consists of:
- Investigate incidents
- Design/model policy change
- Remediate

There are at least 2 advantages of using a comprehensive, market-proven model when designing the security architecture and incident response process:

1. No important element is left behind. If an organization follows the model thoroughly, all important elements of the plan will be covered
2. It is easier to defend the organization in case of regulatory audits or lawsuits. By following proven models, the organizations demonstrate they are using all available best practices in protecting their digital assets.

EDR - a key instrument for incident management

Besides people and processes, tools are a necessary and important part of the incident management plan. Most organizations currently rely on endpoint protection platforms (EPP). EPP software (which evolved over time from what we know as antivirus) are modern solutions that employ the entire spectrum of technologies, starting with signatures and ending with machine learning algorithms, that aim to prevent malware or the execution of an attack on the endpoint infrastructure.

An endpoint protection platform will fight against the first four phases (exploitation) of the attack kill chain. To be effective, the EPP solution must prevent the installation of the component used to carry out the main attack. There is a hot debate these days as to whether Prevention is still a valid endpoint protection strategy. Bitdefender's view on this debate is that prevention is alive and well, and will be a key

endpoint protection technology for years to come. Why? Because it successfully blocks more than 99 percent attacks, leaving a very small number of advanced attacks to be handled by incident response teams.

As a complement for endpoint protection platforms, Endpoint Detection and Response (or short EDR) is built to neutralize an attack in the latter stages: Installation, Command and Control or Actions on Objectives. These 3 later phases are also the attack phases where incident response process is very important.

To enable enterprise security teams to successfully undertake the incident response process and effectively respond to security incidents, Bitdefender developed GravityZone Ultra. It's an easy-to-use, integrated next-gen endpoint protection and EDR platform designed to accurately protects enterprises against the most sophisticated cyber threats. It employs prevention, detection and automatic response and provides clear visibility into suspicious activities as well as one-click resolution capabilities.

GravityZone Ultra helps organizations respond to security incidents

Identify

After completing preparation, the first effective step an organization needs to take in responding to an incident or attack is to identify it early. Bitdefender employs a group of technologies that work together to monitor and record the activity at endpoint level to detect any trace of cyberthreat and suspicious activity. Once a suspicious event or series of events are detected, two courses of actions can follow. If the suspicious actions are clearly identified as threats, automatic containment will immediately follow. No human intervention is required.

On the other hand, if the machine learning algorithm cannot conclude that the suspicious actions are cyber threats, they are registered as incidents and the incident response team is alerted. To further investigate, the security analysts can use a set of instruments that include a graphic representation of the chain of events, contextual information, sandbox outputs or correlations with Virustotal.

For maximum effectiveness, the security incidents are graded by severity and all related information is, by design, accessible to the threat hunter with a single click. The security analyst will use all this information to search for indicators of compromise and to decide as soon as possible if a suspicious activity is a threat or a harmless activity.

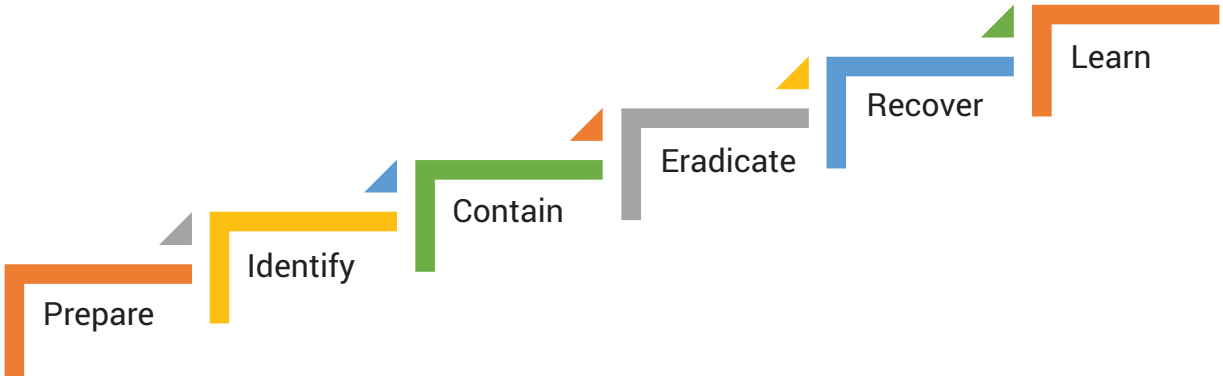


Figure: Incident Management Process

Contain

Once the investigation ends with a conclusion, the identify phase of the incident response process ends and the next phase, Contain, begins. To stop an attack, GravityZone Ultra, contains 2 sets of instruments: automatic and manual. If the detection mechanisms conclude that an incident is a threat, automatic containment mechanisms kick in without any human intervention. They will terminate the process, block access and/or quarantine files if required.

The other set of tools are available for the incident response teams once they manually investigate and decide that an incident was a threat. They can immediately quarantine the endpoint and add the malicious file to a block list. In this way, the attack is prevented from spreading laterally.

Easy-to-use EDR

EDR solutions are notoriously noisy and hungry for analyst's time and attention. GravityZone Ultra was built to reduce the resources and skill requirements for effective incidents response. It leverages industry leading prevention and security automation to sharply reducing the number of incidents requiring manual investigation and provides visualization and context information for easier and faster incident resolution.

Eradicate

Once the attack is stopped, the security team can focus on eradicating all traces of the attack and restoring systems to pre-attack states.

GravityZone Ultra features disinfection and removal technologies that can act very effectively against identified cyberthreats and contain them automatically. For other types of threats, incident response teams can rely on other instruments from simple, generic tools to more complex ones. They can use advanced file managers, registry editors, registry backups, configuration tools and so on.

Recover

The recovery phase's purpose is to fully restore affected endpoints to the pre-attack phase. GravityZone Ultra can automatically roll back changes made by most malware, but additional instruments like backups are very important to have at hand to restore the functionality of endpoint infrastructure.

Data records important for organizations must be always properly backed up. Testing the restore procedure from time to time is also important. In many situations, important IT infrastructure is unavailable for long periods not because of the lack of backups, but because of restoring plans that are not working.

After restoring the functionality of affected endpoints, further monitoring is required for 2 reasons:

- To ensure that the attack is really and fully stopped
- To ensure that restored endpoints are functioning properly

The monitoring and reporting module included in GravityZone also provide information about all activities described above. If required by regulation, this helps teams prepare in due time reports on the security incidents and affected data. This is especially useful for incidents falling under GDPR, as the timeframe to report a personal data incident is limited to 72 hours from detection.

Close the security circle: Learn

The last phase of the incident response process is to learn. The security feedback loop has a few elements attached to it. First is the human element. People learn best from experience and information acquired during the incident handling needs to be structured and spread as lessons learned within the organization.

Second, the learning needs to translate into updated policies and procedures. Typically, legal consequences of data breaches following similar scenarios are more serious, as organizations must avoid the same mistakes.

Third, elevating the security posture of the organization by patching systems identified as vulnerable. One of the major failures in the Equifax case study, was to not have a proper patching policy in place. The GravityZone portfolio includes a Patch Management module that can be attached to all enterprise products. GravityZone Patch Management is designed to enable organizations to keep systems up to date across the entire Windows install base. It can manage software updates for Windows operating systems and for the largest collection of software applications on the market.

Endnotes

1 https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html
2 https://nvd.nist.gov/vuln/detail/CVE-2017-5638
3 https://cwiki.apache.org/confluence/display/WW/S2-045
4 https://www.gartner.com/doc/3723818/use-carta-strategic-approach-embrace

Bitdefender is a global security technology company that provides cutting edge end-to-end cyber security solutions and advanced threat protection to more than 500 million users in more than 150 countries. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a provider of choice in both hybrid infrastructure security and endpoint protection. Through R&D, alliances and partnerships, Bitdefender is trusted to be ahead and deliver robust security you can rely on. More information is available at http://www.bitdefender.com.

FOR MORE INFORMATION VISIT: bitdefender.com/business