Precursors Explained

"Precursors" or "Threat Precursors" are elements of the incident identification and response process that allow both an attacker and a security researcher or professional to determine the existence of flaws and/or vulnerabilities within a system. By identifying precursors organizations can work to prevent cyber attacks before they occur.

ISSUES WITH PRECURSORS

Precursors can help a lot in the security scheme of an organization, but they have a very big disadvantage in terms of identification. This is that they are usually the most complicated element to obtain in a threat identification process. After all, the vast majority of attacks do not have identifiable or detectable precursors (from the organization's perspective); this is undoubtedly a factor that affects the time of detection, and it is such a big handicap, because, if organizations have the knowledge about this type of elements, they could have the opportunity to prevent one or several incidents simply by altering their security posture.

TYPES OF PRECURSORS

Attacks can take many different forms, and attackers can find many ways to compromise a system. With this in mind it is undeniable to admit that precursors can appear in many different ways and above all, both attackers and security professionals can use many tools to obtain them. Some examples will be shown below.

Port Scanning, Operating System and Application Fingerprinting

One of the most effective ways to obtain information about a network is through scanning. Using tools such as Nmap, Netcat or Nessus, both a researcher and an attacker can learn about the services and vulnerabilities that exist on a system. A lot of information can be gained from performing host discovery, port scanning, and vulnerability scanning activities, such as which ports or services are running and responding on a system, what operating system is installed on the system, and what applications and versions of applications are present.

When considering the precursors that this activity would generate, we would mainly be looking to monitor network connections and event logs from internet-facing systems.

- Logs from firewalls or web application firewalls (WAFs) that have rules written to alert and log when one source IP is attempting to connect on X number of ports over a short period of time.
- Logs from systems that are being scanned.

Social Engineering and Reconnaissance

Another way to obtain the greatest amount of information about an organization is, without a doubt, social

engineering. This is because, with social skills and deception, both an attacker and a researcher can learn about any type of information and vulnerabilities of an organization. Techniques such as "dumpster diving" (searching for items in the rubbish such as USB sticks, printed documents, notebooks, etc) or "eavesdropping" (Listen to conversations between employees) are very useful for identifying pieces of information that can be brought together to potentially discover vulnerabilities that can be exploited by an attacker.

When considering the precursors that this activity would generate, we would mainly be looking to listen to employee reports of unusual or suspicious activity, or CCTV footage from both inside and outside the office.

- Non-employees looking through the organization's bins that are conducting 'dumpster diving'.
- Non-employees hanging around outside the office or lobby areas.
- Employees being engaged with outside or near the office by unknown individuals.
- Calls from unknown, withheld, or spoofed phone numbers.
- Documents or office equipment going missing.

OSINT Sources and Bulletin Boards

And finally, we have the review of social media, blogs, forums, and bulletin boards, security articles and reports, and other OSINT data both on the clear web and dark web.

When considering the precursors that this activity would generate, we would mainly be looking to monitor OSINT sources using free tools such as TweetDeck, and paid intelligence resources such as Recorded Future.

- An email or online message from a threat group threatening or stating they will attack the organization.
- Publicly disclosed vulnerabilities (CVEs) that affect systems or programs that are used by the organization.
- Chatter on underground forums about a zero day or new malware that is being exploited or utilized in the wild.
- Reports stating an increase in vulnerability exploitation activity supplied by government organizations or intelligence vendors.

CONCLUSION

Precursors can appear in many forms and security professionals can take advantage of this to improve existing security positions in an organization or in their own system. Every day, attackers try harder to attack and infect their target, and it is everyone's duty to prevent them from achieving their goal.

Previous Topic
Mark Complete
Next Topic
Back to Lesson