Espionage as a Service

Cybercrime as a Service Series

Cybercrime as a service (CaaS) is an important trend in Deep Web forums because it puts cybercriminal tools and services in the hands of a wider range of threat actors—even the nontechnical, such that anyone can become a cybercriminal with minimal investment. At the same time, cybercriminals are now seeing the advantages of expanding their targets from home users to larger enterprise networks. This is a matter that enterprises need to be ready for.

How Espionage as a Service Works

Many discussions on espionage focus on how nation-states steal another’s intellectual property, top-secret plans, and other high-value information via cyber attacks. Enterprises, however, are not exempt from spying. Compared with other much-discussed threats to confidential corporate data or “company crown jewels” such as ransomware and distributed denial-of-service (DDoS) attacks, very few are aware of espionage-as-a-service (EspaaS) offerings in underground markets and the Deep Web that can impact victims’ bottom line.

The United States, for instance, spends more on research and development (R&D) than any other country worldwide. Developing unique offerings to gain a competitive edge requires a lot of effort and resources. Economic espionage can cost the United States alone billions of dollars each year. While it is not new, it is growing, and theft attempts by competitors and adversaries are becoming more brazen and varied.

Attackers can easily obtain espionage tools and services underground to spy on and steal company crown jewels that they can then sell to the victims’ highest-bidding competitors or use to further line their pockets via extortion. Bidders could be seeking competitive or strategic advantages over rivals or disgruntled former employees who wish to take previous employers down.

Some espionage-as-a-service offerings available underground include database-, Web-server-, website-, and email-hacking services; doxing (gathering data otherwise not publicly available on a chosen individual or company) services; and hacking tutorials and spying tools.

The huge amounts of money that individuals and companies shell out to get their hands on rivals’ crown jewels entices an increasing number of cybercriminals to peddle espionage-as-a-service offerings. The fact that hackers are very hard to track and apprehend, and that related tools and services are easy to provide and procure, is contributing to the proliferation of espionage as a service. Law enforcement agencies would much rather focus on capturing nation-state actors as well, further decreasing risks to cybercriminals engaging in the business.
What This Means for Enterprises

We have seen governments and public agencies succumb to nation-state espionage attacks. Enterprises have to keep in mind, however, that all companies, regardless of industry and size, can fall prey to espionage attacks.

Companies in the United States can, according to a 2015 ITProPortal study, lose a whopping US$300 billion to intellectual property theft each year. In the United Kingdom, meanwhile, a 2011 Detica report pegged the total cost of cybercrime at £27 billion each year. Some £9.2 billion of the said amount could be attributed to intellectual property theft while £7 billion accounted for losses due to corporate espionage.

Corporate espionage can cause a company to lose highly confidential assets such as blueprints, patents, product designs, works in progress (technologies, products, or services in development), unique processes, and mergers and acquisitions (M&A) data, among others that can affect its bottom line. Other effects include:

- Loss of competitive edge over business rivals
- Brand and reputation damage
- Loss of potential profits from technologies, products, or services in the works
- Dwindling financial resources due to the payment of huge attack-recovery costs

There exists a very thin line between targeted and EsaaS attacks; the latter just has an extra step. They essentially employ the same tools, tactics, and techniques. The EsaaS attack chain comprises the following components:

- **Conduct reconnaissance:** Attackers gather intelligence on intended targets. They look at targets’ network infrastructure and company structure to identify who in the organization to go after in order to get the data they want to steal. At this stage, targets’ crown jewels are identified.

- **Identify entry point:** Using the intel, attackers send a contextually relevant malware-laden spear-phishing email to bait the target. Social engineering ploys play a crucial role in how successful a spear-phishing campaign is. Attackers usually target high-ranking corporate officials in a technique called ‘whaling’ as obtaining their credentials can open more doors than going after typical employees.

- **Infiltrate network:** Attackers establish command and control (C&C) over target networks aided by malware such as backdoors, remote access Trojans (RATs), and, at times, even Trojan spyware.

- **Achieve lateral movement:** Once attackers gain a foothold in target networks, they need to remain persistent while moving laterally until they infiltrate systems where the company crown jewels are actually stored.

- **Exfiltrate stolen data:** Once the company crown jewels are located, attackers need to exfiltrate or transfer stolen data without triggering security alarms to locations only they can access.

- **Sell stolen data to the highest bidders (usually business rivals) or extort money from victims:** This is an additional component for EsaaS attacks. Targeted attacks typically stop with data exfiltration, but because EsaaS attacks are considered a form of cybercrime, the last step always involves profits. Buyers of the stolen data may, of course, be pre-identified, as is the case with hackers for hire.
This strategy combines gateway, network, and endpoint protection that:

- Shields systems, devices, and the network from known and “unknown” threats (new or improved malware versions and zero-day exploits)
- Only allows “good” (nonmalicious) files and applications to run on systems and devices
- Ensures system and network integrity by making sure that unexpected and unwanted activity is not present
- Keeps systems and devices secure even if the network perimeter is compromised
- Isolates threats detected on systems and devices so they will not compromise the entire network

References: