http://www.telecomkh.com/en/internet/products-and-services/9118
Javelin Networks unveils the attacker decision tree
07/06/16

Date: ***Wed, 06/07/2017 - 14:09*** Source: Javelin Networks

How advanced persistent threats (APTs) take shape

Greg Fitzgerald, Chief Operating Officer & Chief Marketing Officer, Javelin Networks, at the NetEvents European Media Spotlight "Innnovators in cloud, IoT, IA & Security", London

PHOTO / telecomkh.com

Javelin Networks is a cyber security company created by security operators/hackers to defend against criminal security operators. The founders at Javelin expose ‘military secrets,’ as they themselves were extensively trained about how attackers create an Advanced Persistent Threat (APT) following their years of work on the inside.

Hacker’s Decision Tree

It is inevitable that a computer is going to get compromised. A foothold will be established in one of the victim’s machines. Yet, once the foothold is made, attackers have limited options. The key is to create an attack that enables reuse of the APT over and over internally, or even to other victims externally, without detection.

“APT is an operation,” and attackers are seeking information. Information permits them to violate trust. Trust of the computer, the applications, the people, and their permissions. It allows attackers to remain stealthy for as long as possible. But there is one factor most critical to the operations: budget. Hacking is a business,

and at the end of the day, it's all about return on investment (ROI). For each step an attacker makes, there is a decision on risk of detection, cost to pursue and time.

Therefore, in addition to being stealthy and quiet for a long time, we also need to be efficient. There are only two types of "FOOTHOLDS" an attacker can use: The first type being a foothold with corporate domain access or without domain access. Call this the four obvious reasons:
1. Attackers can encrypt targets from within the corporation (potentially all of them), and then ask for a big ransom, also not before we make sure we disabled the endpoint protection
2. Attackers can also just steal data.
3. Attackers can cause damage to the environment.
4. Try to control their cloud infrastructure/ SaaS apps… Yes. from within the corporate domain.

Those are the four obvious reasons. The other not-so-obvious one is to create a backdoor, mainly in a way of corporate domain persistence, so if something goes wrong, the attacker will still be able to go back to the environment and continue the attack.
As an industry, we spend billions (greater than $85B to be more precise) on protection, detection, response, and education, yet the rate of breaches is higher than ever before. But if one considers the real abilities and behaviors of attackers, this daunting task of keeping an organization safe is manageable. Common knowledge is that any computer or device can be compromised, no matter how much protection is bought. Someone will eventually click on a link they shouldn't, visit an infected web site, open an injected document, etc. Hackers have the time, resources, and skill to always hijack a computer. Once the machine is compromised, however, the attacker is limited in their options to move around.
Even in the most advanced attacks, the hacker will not immediately know whose computer they have access and privileges for, what computers are around them, what detection technologies are present, etc. He must discover these things.

Discovery
This discovery provides the attacker with contextual awareness of where they are and how they can proceed to penetrate past the point of compromise into the organization. An 'Attacker's Creed' is to establish presence, move undetected, and maintain persistence. After all the work of establishing a foothold, the last thing an attacker wants is to be detected and stopped. The cost to the attacker to gain access is as meaningful as what the defender spends on defense technologies.
Interestingly, attackers can perform discovery from the compromised machine in

only 3 ways:

1. LLMNR DNS Query
2. Network Scan
3. Active Directory Query

1. Link-Local Multicast Name Resolution (LLMNR) is a protocol based on the Domain Name System (DNS) packet format that allows both IPv4 and IPv6 hosts to perform name resolution for hosts on the same local link. It gives the attacker knowledge of the computer(s) it can access in the segment in which it resides. Downside: The information that's provided is limited. Just knowing the computers around them does not give attackers all the information about applications, services, users and credentials they need. There is no additional information the attacker needs, like user, permissions, passwords. There is also no validation whether this computer is real or a possible honeypot.

2. Network scanning is a procedure for identifying active hosts on a network, either for the purpose of attacking them or for network security assessment. Scanning procedures, such as ping sweeps and port scans, return information about which IP addresses map to live hosts that are active on the Internet and what services they offer. Another scanning method, inverse mapping, returns information about what IP addresses do not map to live hosts; this enables an attacker to make assumptions about viable addresses.

Downside: This is also a practice by attackers and IT administrators to know what computers are on a segment. However, it's limited too. Its 'noisy' to other monitoring/detection systems and time consuming. Like LLMNR, this effort too only gives presence information, no other detail that helps the attacker know the vulnerabilities, apps, or credentials.

3. Active Directory is a Microsoft infrastructure component that is just a database. It houses every computer, user, credential, group policy, service, application, and mapped detail of an organization's IT topology. By design, for easier IT operations management, it can be queried for any of this information by any computer connected to the Directory—making it the primary database attackers use to get ALL the information they need. It's the only place to run!

Downside: None.

Moving Laterally

Once attackers have reconnaissance information, they can move laterally around the network as they wish. However, to move laterally off the compromised machine to another computer undetected, they only have 2 options:

1. Jump from computer to computer using unpatched vulnerabilities
2. Steal valid domain credentials that permit them access without alarms

Unpatched vulnerabilities are difficult to find. Most people call them ‘zero days’, as detection and prevention technologies don’t have prior knowledge about them and don’t have a signature to protect systems. They are rare, costly, and require lots of resources to find and ultimately exploit.

Domain credentials, on the other hand, are easy to find. They are stored in the organization’s internal network infrastructure and can be extracted using many common tools and techniques. These are simple to access and require very few resources to obtain. For this reason, stealing valid domain credentials is the easiest and least detectable way for attackers to move around.
Of the 3 discovery methods and 2 movement methods, the most viable activity with the least risk, cost, and time to the attacker is querying Active Directory for discovery and stealing domain credentials for movement. This is a proven strategy as demonstrated by every major successful attack in the past 5 years using domain credential theft, Active Directory reconnaissance, and lateral movement—whether it’s APT10, APT28, SAMAS Ransomworm, Duqu, etc.

Javelin AD|Protect
Javelin is designed to detect the attacker at their point of compromise and block them from gaining the reconnaissance information that will permit them to penetrate further onto other computers and into the network. Javelin is an endpoint, ‘agentless’ solution that obfuscates attacker queries to an Active Directory.
It presents the attacker with a false reality of the information they collect, giving away their presence, their tradecraft, and pathway. Javelin automatically identifies, detects and initiates protection methods that quarantines the attacker on the compromised computer and evicts them from the domain. Concurrently, it provides immediate patient zero data and exact forensics activity about the attacker (i.e. whether this is a one-time, one computer attack, a larger campaign, or a remnant of a past compromise). Javelin fills the gap between prevention and the laborious, time-delayed effort of detection and response.