Fileless malware' attacks

Fileless malware attacks, which were recently discovered in the networks of at least 140 banks, telecoms and governments, account for about 15% of known attacks today and have been around for years in different forms. "Fileless malware attacks are becoming much more common and circumvent most of the endpoint protection and detection tools deployed today," Gartner security analyst Avivah Litan said.

A recent discovery of fileless malware was reported on Wednesday by researchers at Moscow-based Kaspersky Labs. The attackers have not been identified and "attribution [is] almost impossible," according to Kaspersky. Called "fileless malware" attacks because the malware resides only in memory and is mostly hidden, these exploits have been used by unknown cyberthieves to steal from ATMs and customer accounts. However, the full extent of damages isn't always known.

The latest threat was originally discovered by an unnamed bank's security team that found malicious code inside the physical memory of the bank's domain controller, a kind of server that responds to security authentication requests. The unnamed banks and other organizations that have been infected reside in 40 countries, with five nations, the U.S., France, Ecuador, Kenya and the U.K., the most affected. There were 21 attacks on organizations in the U.S., Kaspersky said.

While the objectives aren't fully known, the attackers have targeted banks' computers to siphon money out of ATMs, according to Kaspersky Labs researcher Kurt Baumgartner in a report by Arstechnica. "Thieves use this for all kinds of attacks, including stealing cash from ATMs and stealing money from accounts," Litan said in an email. "Over half of the financial breaches Gartner has seen against banks and retailers in the past two years use these techniques."

She said the attackers in the now-famous hack on the Target store chain in 2014 relied in part on fileless malware to gain access to systems. Litan advised companies to take several steps to prevent or quickly detect fileless malware attacks:

* Patch systems often to avoid the most common vulnerabilities.
* Restrict the use of administrative tools like Microsoft PowerShell to just a few endpoint computers and users based on their "need to have" the use of the tools.
* Invest in products that include protection against in-memory attacks.
* Symantec, Trend and McAfee are adding them.
* Consider using application controls on endpoint computers so only an organization's permitted applications can run.

ATMs and customer accounts

The latest threat was originally discovered by an unnamed bank's security team that found malicious code inside the physical memory of the bank's domain controller, a kind of server that responds to security authentication requests. The unnamed banks and other organizations that have been infected reside in 40 countries, with five nations, the U.S., France, Ecuador, Kenya and the U.K., the most affected. There were 21 attacks on organizations in the U.S., Kaspersky said.

While the objectives aren't fully known, the attackers have targeted banks' computers to siphon money out of ATMs, according to Kaspersky Labs researcher Kurt Baumgartner in a report by Arstechnica. "Thieves use this for all kinds of attacks, including stealing cash from ATMs and stealing money from accounts," Litan said in an email. "Over half of the financial breaches Gartner has seen against banks and retailers in the past two years use these techniques."