Fileless Memory-Based Malware Plagues 140 Banks, Enterprises

Author:
Chris Brook

February 8, 2017
/ 4:37 pm

2:30 minute read

Share this article:

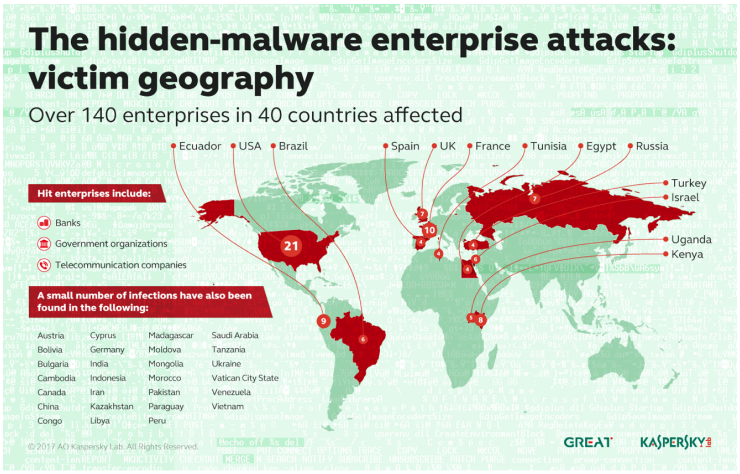
Attackers have been using fileless malware to hide in the memory of enterprises, steal data, and vanish without a trace.

Attackers have been using well-known, standard utilities to carry out attacks on organizations around the world, and covering their tracks by wiping their activity from the machine's memory before its rebooted.

The attackers, who may be connected to the GCMAN and Carbanak groups, aren't using signature-based malware to carry out their attackers, instead they're using fileless malware hidden in the memory of the affected servers.

Researchers with Kaspersky Lab's Global Research and Analysis Team described the attacks Wednesday in a blog post on Securelist.

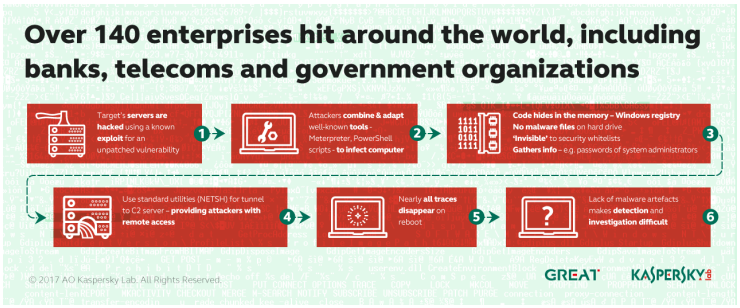
More than 140 enterprises–primarily banks, government organizations, and telecommunications firms in 40 countries, including the U.S., France, and Ecuador–have been affected, according to Kaspersky.



Researchers uncovered the attacks after banks in the Commonwealth of Independent States found Meterpreter, an extensible payload component used by Metasploit, inside the physical memory of a domain controller. Researchers with Kaspersky Lab found the software had been combined with PowerShell scripts in order to invisibly siphon up the passwords of system administrators.

Once they got this information, the researchers claim the attackers essentially had remote access to the machines. They were also spotted using another legitimate utility, Microsoft's command-line scripting utility NETSH, to funnel traffic from the victim's host to the attacker's command and control system.

Researchers believe attackers used Mimikatz, an open-source, post-exploit utility, to grab credentials for service accounts with admin privileges. After achieving admin privileges, they could use NETSH and another Microsoft utility, SC, and carry out the usage of malicious PowerShell scripts.



While researchers were able to determine the techniques used in the attacks; narrowing down who exactly carried them out is difficult given they were carried out with everyday tools and how skilled the attackers are at evading detection.

"The determination of attackers to hide their activity and make detection and incident response increasingly difficult explains the latest trend of anti-forensic techniques and memory-based malware," Sergey Golovanov, Principal Security Researcher at Kaspersky Lab said Wednesday.

"That is why memory forensics is becoming critical to the analysis of malware and its functions. In these particular incidents, the attackers used every conceivable anti-forensic technique; demonstrating how no malware files are needed for the successful exfiltration of data from a network, and how the use of legitimate and open source utilities makes attribution almost impossible."

It's unclear how victim enterprises had their servers hacked in the first

place. According to researchers, the attackers used a known exploit for an unpatched vulnerability.

Golovanov and Igor Soumenkov, another researcher with the company's GReAT team plan to present additional details around the operation – including a second part, how attackers extracted money from banks via ATMs – in April, at the Kaspersky Lab Security Analyst Summit.

While researchers claim they're unsure who's behind the attacks, they said their approaches do bear a resemblance to groups previously uncovered by Kaspersky Lab, such as GCMAN and Carbanak.

Like these attacks, GCMAN, a group the firm described at the Security Analyst Summit last year, used legitimate pen-testing tools, like Meterpreter, to target banks. Once inside a network, they pivoted, bouncing around from machine to machine until they could transfer money from a bank computer to e-currency services. Attackers managed in one instance to transfer $200 payments per minute to a money-mule account without the bank being any the wiser.

Details around the Carbanak gang, a group of attackers who purportedly stole $1 billion from 100 banks, emerged at the Security Analyst Summit in 2015. In that campaign attackers used a one-two punch of a spear-phishing email and a backdoor to manipulate access to banking networks and steal money.

Over the last few months the group has reemerged and been seen shifting its gears, in November 2016 it began targeting the hospitality and restaurant industry. Last month it was learned the group was using Google hosted services for its command and control channels.

Malware Security Analyst Summit